Cybercrime and Online Safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users— A Case of African States

VITUS, Emmanuel Nnaemeka

Graduate, Department of Local Government and Development StudiesObafemi Awolowo University, Ile Ife Osun State

Abstract—

The internet has made the world more linked than ever before. While taking advantage of this online transition, cybercriminals target flaws in online systems, networks, and infrastructure. Businesses, government organizations, people, and communities all across the world, particularlyin African countries, are all severely impacted on an economic and social level. Many African countries focused more on developing secure electricity and internet networks; yet, cybersecurityusually receives less attention than it should. One of Africa's major issues is the lack of adequate digital security infrastructure, which has harmed businesses, governmental institutions, and individual communities more than it has helped. The majority of African countries operate without cybersecurity measures in place to combat cyberattacks. Only a few examples of today's cyber risks include digital extortion, business email intrusion, data breaches, online fraud, ransomware,and phishing, and new types of cybercrime are always developing. Due to the advent of new technology, cybercriminals have become more organized and quicker in their attacks and alliancecreation. To maintain a secure digital environment for all internet users, this study focused on thechallenges, solutions, and need for African countries to improve their online safety by tackling cybercrime, online fraud, and cybersecurity concerns. The objective of this study is to offer practical and long-term answers to the problems posed by cybercrime, with a continuing emphasis on enhancing online safety. It will assess the effectiveness of cutting-edge cybersecurity measures, legislative frameworks, and cross-border cooperative efforts, as well as potential areas for improvement. Additionally, the study will examine cutting-edge methods like blockchain technology, machine learning, and other cutting-edge methods that could improve our using digitaldefences to stop cybercrime.

Keywords — Cybercrime, online safety, cyber security, safe digital environment, internet, socialmedia, privacy, cyber laws, online fraud

1. Introduction

The Internet is a **global network** of interconnected computers and other electronic devices. The Internet allows you to access nearly any information, contact anybody on the globe, and do a lot more. All of this is possible simply by connecting a computer to the Internet, generally known asbrowsing online. When someone says a computer is online, it simply means it is linked to the Internet. The Internet is one of the most crucial aspects of modern life. The internet now serves two primary purposes thanks to the information technology revolution. On the one hand, it has given the world positive contributions. However, it has also resulted in several issues that undermine social order and have given rise to a fresh wave of crime around the globe.

The Internet is used for a variety of reasons, depending on the needs of the user, such as communication, research, education, financial transactions, threading, etc. The internet has evolved into a haven for the most profitable and risk-free criminal activity. This research focuseson cybercrime or e-crimes (electronic crimes), another term for cybercrime. It refers to criminal activity that involves the internet, a computer, or other electronic devices (Alex Roney Mathew, Aayad Al Hajj, and Khalil Al Ruqeishi, 2010).

Cybercrimes are offences that are committed against individuals or groups with a criminal motiveof intentionally harming the reputation of the victim, causing physical or mental harm, and causingloss of money or information directly or indirectly by using the Internet and electronic devices (Johnson, 2013), (Broadhurst R. & Grabosky P., 2005), (Alex Roney Mathew, Aayad Al Hajj, andKhalil Al Ruqeishi, 2010).

Cybercrimes are increasing in frequency and causing extensive damage to governments, companies, society, and individuals (Broadhurst R. & Grabosky P., 2005). Moreover, cybercriminals are motivated in various ways, including (but not limited to) financial gains, emotional instability, societal norms, and lack of legislation and punishment.

Due to the advancement of information technology and software modifications, there is an annual rise in Cybercrimes (Rekouche, 2011). As a result, Cybercrimes are now increasingly prevalent and spread through a variety of means, such as harmful programs that are designed specifically topenetrate personal computers (PCs) or business networks.

Computer systems for deleting systems or duplicating private data. Hacking, Phishing, Spamming,Identity theft, Cyberstalking, Cyber defamation, Cyber terrorism, Cyptojacking, Denial of serviceattacks, and Malware are the most well-known of these techniques. (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013) (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009).

Africa exceeds other regions including North America, South America, and the Middle East in terms of Internet users with over 570 million in circulation. Considering the faster digitalization, the variety of users as a percentage of the population equals roughly 43.1%, suggesting that the number is anticipated to increase in the upcoming years (Statista, 2023). Kenya, with 83% of its population online, Nigeria, with 60%, and South Africa, with 56%, are the top three nations. In each of these countries, mobile banking specifically is acknowledged to be widely used, which contributes to Africa's active engagement in digital financial services.

With the proliferation of malicious apps on mobile devices exploiting growing weaknesses, it poses a serious concern in the future. The technological divide continues to be an issue despite theincreased demand for online mobile banking, particularly as member nations in Africa advance inintegrating digital infrastructure into the pillars of their society, including government, banking, business, and essential infrastructure. This change emphasizes how critical it is to ensure that cybersecurity guidelines and standards satisfy the current and future expectations of this community, especially the need for financial inclusion.

2. Objectives of The Research

This research sets out to explore the unique challenges and solutions to cybercrime and online safety within the context of African society. By focusing on the specific nuances and dynamics ofthe African digital landscape, this study aims to uncover the intricacies of cyber threats faced by individuals, organizations, and governments in the region while identifying effective measures tocounter them.

Furthermore, this study aims to examine the existing legal and regulatory frameworks in African countries concerning cybercrime and online safety. It will evaluate the effectiveness of these frameworks in deterring cybercriminal activities, protecting individuals' digital rights, and fostering a secure online environment. The research will also explore the challenges faced in enforcing cybersecurity laws and the potential for regional and international cooperation in addressing cyber threats collectively.

With a strong emphasis on proactive measures, this research seeks to identify innovative solutionstailored to the African context. It will explore the potential of capacity-building initiatives, public-private partnerships, and cybersecurity awareness campaigns as means to enhance online safety. Additionally, the study will investigate the role of technology in combatting cybercrime, such as the use of advanced threat intelligence systems, data analytics, and incident response mechanismsthat can be adapted to African environments.

By engaging with policymakers, law enforcement agencies, industry experts, and civil society organizations, this research aims to propose actionable recommendations for enhancing cyber resilience in Africa. It will highlight the importance of collaboration between various stakeholdersin strengthening cybersecurity capabilities, fostering digital literacy, and developing sustainable strategies to mitigate cyber risks. The study also aims to provide insights into the potential economic, social, and political impact of addressing cybercrime and improving online safety, emphasizing the benefits of a secure digital ecosystem for Africa's sustainable development.

Moreover, this research endeavours to contribute to the knowledge base on cybercrime and onlinesafety within African society. By identifying the region's specific challenges and proposing tailored solutions, it aims to empower African businesses, governments, and individual communities to navigate the digital realm securely, fostering a resilient and prosperous digital future for Africa.

3. Theoretical Framework

According to Khan (1999), the theoretical framework of the study is a structure that can hold or support a theory of research work. It presents the theory which explains why the problem under study exists. Thus, the theoretical framework is but a theory that serves the alienation of the majority for the benefit of the elites; a segment of disadvantaged citizens who are in the majority have taken to alternative means to survive.

3.1 The Theory of Technology-Enabled Crime

The key insight into the theory is that it combines several categories of criminological theories tohelp society better understand why crimes co-evolved with computer and telecommunications technologies to become among the most complex and difficult forms of crime to prevent,investigate and control. McQuade (1998) reveals that understanding and maintaining relatively complex crime is initially quite difficult, and there is continual competition between criminals andlaw enforcement for technological advantage. As criminals do something new and innovative, lawenforcement must catch up to avert, control, deter, and prevent new forms of crime.

3.1.2 McQuade (2006) argues that technology-enable crime theory encompasses:

1. Crimes are committed directly against computers and computer systems.
2. Activities that fall under this category are often referred to as high-tech crimes, computercrimes, or cybercrimes.
3. The use of technology to commit or facilitate the commission of traditional crimes.
4. Crimes such as fraud, scams, and harassment can be facilitated using technology whichbrings unique challenges to old crimes.

The theory provides a framework for analyzing all types of crime, particularly those that are emerging as a result of inventions and advancements in computing and telecommunications technologies. The idea is relevant for comprehending current challenges posed by developing kinds of cybercrime, international crime, and terrorism networks that defy established criminal justice and security mechanisms for preventing and managing crime.

The idea is pertinent to our study because it gives us insight and comprehension into the new toolsand tactics employed by cybercriminals; that is, a transition from a basic crime performed with simple tools to a complex crime committed with sophisticated instruments. It also aids incomprehending new types of deviance, social abuse, or crime done via the creative application oftechnology.

4. Conceptual Clarification

4.1 Cybercrime: cybercrime, also called computer crime, is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. (Encyclopedia Britannica, 2023 Edition)

4.2 Online safety: Online safety is the ability to understand and recognize threats that exist on theinternet, as well as having the skills and knowledge to avoid these threats. This includes knowinghow to keep personal information private and secure online, protecting devices from malware, avoiding harmful or illegal content, and managing online relationships safely.

4.3 Cyber security: One of the difficulties of online safety is that the threats are constantly changing, and getting ever more sophisticated. However, when teaching students online safety skills, there are some basic concepts that, when mastered, can help prevent a wide variety of threats. These include: Securing and protecting personal information such as Full name, Address, School or work, Social security number, Account usernames, and passwords. Students should be taught never to share personal information online without a parent or guardian's specific permission. They should also never share the usernames and passwords of their accounts, which may be used to obtain personal information.

4.4 Internet: It's an electronic communications network that connects computer networks and organizational computer facilities around the world used with *the* except when being used attributively. It is also a communications system that connects computers and computer networksall over the world. The first known use of the "Internet" was in 1986 (Merriam-Webster Dictionary, 2023 Edition)

4.5 Social media: forms of electronic communication (such as websites for social networking andmicroblogging) through which users create online communities to share information, ideas,personal messages, and other content (such as videos)

4.6 Privacy: An individual or group can seclude themselves or information about themselves, andthereby express themselves selectively. The domain of privacy partially overlaps with security, which can include the concepts of appropriate use and protection of information. Privacy may alsotake the form of bodily integrity. There have been many different conceptions of privacy throughout history. Most cultures recognize the right of an individual to withhold aspects of theirpersonal lives from public records.

4.7 Cyber laws: Cyber Law is generally termed as "Law of the Internet" or "IT Law." It's a legalaspect that oversees issues relating to the Internet, computing, cyberspace, and other related matters. As the web of the internet and technology become more woven into our lives, so are the complexities of information and our vulnerability to hacking, ransom, and other crimes. Cyberlawacts as a protection over cyberspace, preventing cybercrime from happening. Cyberlaw serves as one of the emerging aspects of the Nigerian Legal System. This is a result of the rapid advancementof Internet technology. People who engage the internet have legal safeguards under cyber law. This covers both business and common citizens. (Chamber Law Firm, 2022)

4.8 Online fraud: Online fraud also known as Internet fraud, is a sort of cybercrime that involvesdeceit and the use of the Internet. It may entail the concealment of facts or the provision of false information to defraud people of their hard-earned cash, assets, and inheritance. Internet fraud is aterm used to describe a variety of unlawful and criminal activities carried out online rather than asingle, separate crime. It differs from stealing, though, in that the victim in this instance knowingly and deliberately gives the offender the property, money, or personal information. Another aspect that sets it apart is the fact that it includes offenders who are separated in time and space.

5. Cybercrime and Online Safety

5.1 Cybercrime

Cybercrime is a criminal activity that is done by using computers and the internet including anything from illegal downloading of music files and games to stealing millions of dollars from online accounts (Gorazd Mesko, and Igor Bernik, 2011). Also, non-monetary offences, such as creating and distributing viruses on other computers or posting confidential business information on the internet through music and game files. (Schaeff B, Chan H., and Ogulnick S., 2009).

5.1.1 Impact of Cybercrimes

Cybercrimes affect the community in many ways. This includes (Amber Stabek, Paul Watters, andRobert Layton , 2010) (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013)(Balkhi, 2013) (Brokenshire, 2013):

1. Loss of online business and consumer confidence in the digital economy,
2. The potential for critical infrastructure to be compromised affecting water supply, healthservices, national communications, energy distribution, financial services, and
3. transport,
4. Loss of personal financial resources and subsequent emotional damage.
5. Loss of business assets,
6. Costs to government agencies and businesses in re-establishing credit histories,
7. accounts and identities,
8. Costs to businesses in improving cyber security measures,
9. Stimulating other criminal activity, or
10. Costs in time and resources for law enforcement agencies.

Cybercrime encompasses a broad range of actions and conduct. At one end are offences involvingfundamental invasions of individual or corporate privacy, such as attacks on the accuracy of data stored in digital repositories, identity theft, and the use of illegally obtained digital information toblackmail a company or person. Transaction-based crimes including fraud, pornography, digital piracy, money laundering, and counterfeiting fall in the middle of the range.

These are individual crimes with specific victims, yet the perpetrator remains hidden and unseen but with due consideration on the part of the Internet's relative anonymity, most of these fraudstersare brought to justice. Data tampering is another part of this sort of crime, which is done on purposefor monetary gain, individual gain, or political goals. Crimes that entail efforts to commit a crimeare at the opposite extreme of the range. These include spamming, hacking, and denial of service attacks against specific sites to acts of cyber-terrorism by non-state actors—that is, the use of the Internet to affect a nation's economic and technological infrastructure and cause public disorder ordisturbances and even death (Broadhurst & Chantler 2006).

5.1.2 Methods of Cybercrimes

These are various illegal methods of cyber-crimes that are used by malicious internet users to harmbusinesses, governmental organizations, or individual communities (Bashir, Adil & Shoukat, Saba, 2018)

1. **Cyber Stalking and Harassment**

This is a new type of cybercrime wherein a person's online actions, which contain sensitive information, are compiled and then exploited by the cybercriminal to harass the victim. Women who are stalked by males and children who are stalked by adult predators account for the majorityof victims in this crime. Cyberstalkers use chat rooms, websites, email, and other methods to annoy their victims.

2. **Intellectual Property Crime**

Software, copyright, trademark, and other types of intellectual property are all examples of intellectual property. Intellectual property rights are allegedly breached or denied whether they are done so partially or whole. Additionally, any illegal activity that denies a property's owner all or part of their rights is a felony, including software piracy, trademark infringement, copyright infringement, patent infringement, and design infringement.

3. Phishing

It's a method that hackers employ to steal private data, including credit card information, usernames, passwords, PINs, bank account numbers, and other details. Phishing is frequently carried out using email spoofing, which is the use of false emails that ask the user to provide certaininformation.

4. Cyber Defamation

A person's reputation or image being damaged is considered defamation. Cyberdefamation is theact of committing such an offence utilizing virtual media. It is possible to accomplish this by stealing a person's email account and sending emails to known or unknown recipients using rude or abusive language.

5. Cyber Vandalism

Vandalism is the unauthorized destruction or damage of another person's or group's property. Destruction of data or information on a computer or cloud server is a sort of cyber vandalism. It simply refers to maliciously removing, editing, or adding content to someone else's stuff online.

6. Hacking

One of the biggest risks in the world today is hacking, which has cost many people andorganizations a great deal of money and caused significant societal harm. The number of hackingattacks is rising alarmingly. Hackers are divided into three categories: black-hat hackers, who operate illegally, white-hat hackers, who are moral hackers hired by an organization on a contractbasis to check computer system vulnerabilities, and grey-hat hackers, who work to increase systemand network security. Blue-hat hackers are independent of computer security consulting businesses, and they break into systems without authorization to expose their owners to security flaws. Script Kiddies, Elite Hackers, Hacktivists, and Phreakers are more categories of hackers.

7. Cyber Extortion

It includes the theft of sensitive information and the threat to make it public in exchange for payment to prevent or stop the assault.

8. Cyber Terrorism

It is a terrorist act carried out electronically against citizens, companies, organizations, and even the government itself. For instance, a straightforward email spreading the news of a bomb attackmay be categorized as cyber terrorism.

9. Password Sniffing

It's a method, cybercriminals employ to decipher user passwords. Cybercriminals employapplications called password sniffers to observe and capture the username and password of network users as they check in to a website.

10. Denial of Service Attacks

It is an attempt to temporarily or permanently prevent people from accessing a system or network. When a computer receives more requests than it can manage, it happens. This kind of assault cancause systems to hang. Target websites are often those hosted by banks, payment processors for credit cards, etc.

11. Virus Attacks

Viruses are self-replicating programs that destroy other systems and programs. Emails constructedso the recipient is persuaded to open the email's attachment might propagate viruses. Systems become infected when the attachment is opened and the virus is activated. Thus, by slowing downthe network, these infections interfere with computers' ability to operate properly.

12. Child Pornography

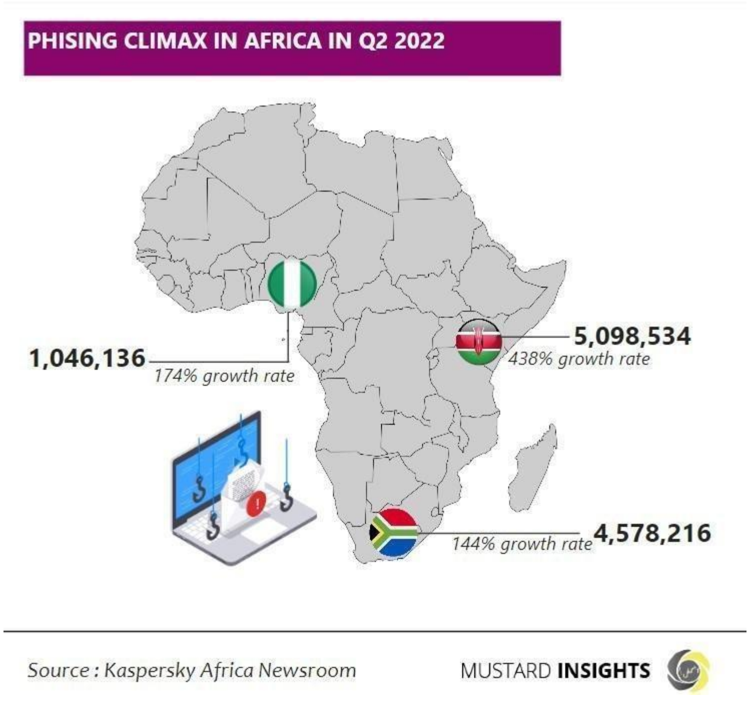
It entails the use of the internet to produce, share, or access content intended to sexually exploit minors.

13. Data Diddling

It is one of the first and easiest ways to commit crimes with computers. It entails altering the databoth before and during entry into the computer system, as well as after processing is complete. Through a virus, it may be transmitted electronically.

5.1.4 African Countries Battling with Cybersecurity Tension Emerging from Cybercrimes

Kenya, South Africa, and Nigeria have emerged as the three African countries with the most phishing attacks in the second quarter of 2022.



Source : Kaspersky Africa Newsroom

Figure 1: KASPERSKY AFRICA NEWSROOM ON PHISHING CRIME IN AFRICA 2022

Following data provided by cybersecurity firm Kaspersky, the three African nations with the mostphishing assaults are Kenya, South Africa, and Nigeria. According to Kaspersky, "attacks relatedto data loss threats (phishing and social engineering scams) increased significantly in Africa in Q22022 compared to the previous quarter."

Social engineering is a trickery method that takes advantage of human negligence to get sensitiveinformation, access, or assets. These "human hacking" schemes in cybercrime tend to entice unwary individuals into disclosing data, spreading malware infections, or granting access to restricted systems. Attacks can occur online, in person, or through other contacts (Kaspersky).

According to the KnowBe4 African Report 2019, phishing was one of the top cyber dangers facedby the African continent, with over "800 respondents across South Africa, Kenya, Nigeria, Ghana,Egypt, Morocco, Mauritius, and Botswana." 28.14% of respondents said they had previously clicked on a phishing email, 27.71% said they had fallen for a scam, and 19% said they had forwarded a spam or fake email." Kaspersky identified around 2 million phishing attempts in SouthAfrica, Kenya, Egypt, Nigeria, Rwanda, and Ethiopia alone in 2020.

5.1.4.1 Kenya, South Africa, And Nigeria Have the Highest Number of Phishing Attacks

Kenya was recognized as the country with the most phishing assaults in Africa, with a total of 5,098,534 million documented phishing attacks - a 438% increase over the first quarter of 2022. This follows allegations that cybercrime in Kenya had climbed to "nearly 140 million in 2020." Malware is the most commonly reported online crime in the country, with an increase of nearly 40% over the previous year" (Statista).

In Kenya, an assault targeted marketplaces and related computer systems, prompting INTERPOLto warn that supply chain attacks might define the cyber security environment in the following decade. Customers in Kenya are particularly affected by high-profile supply chain assaults, such as the breach of the Kaseya IT service by the ransomware organization REVIL34 (Interpol).

South Africa had the second-highest number of phishing assaults in Africa, with 4,578,216 millionattacks - a 144% increase over the first quarter of 2022 statistics. According to Surf-shark statistics,South Africa is the sixth most afflicted country in the world in terms of cybercrime, with an estimated 52 victims per 1 million internet users. In 2021, there were an average of 97 victims perhour, while back in 2001 only 6 South Africans per hour fell victim to cybercrime."

Life Healthcare, South Africa's second-largest private hospital operator in charge of delivering digital services in hospitals throughout Southern Africa, was targeted by a cyberattack in June 2020. During the COVID-19 epidemic, an assault was launched against its admission systems, business processing systems, and email servers, forcing several systems down. It is estimated thatthe organization lost more than a month due to the epidemic (Interpol)."

Nigeria was identified as the third African country with the most phishing assaults, with 1,046,136million attacks recorded - a 174% rise over the first quarter. Despite having the lowest number ofassaults within the group, Nigeria appears to have the biggest number of scammers in Africa. According to a 2020 study from Agari's Cyber Intelligence Division (ACID), "the majority (60%)of BEC actors globally were located in Africa, across 11 countries in the region," with Nigeria accounting for "83% of African attackers, as well as 50% of global BEC actors."

Furthermore, "in November 2020, three Nigerian nationals were believed to be members of a largerorganized crime group responsible for distributing malware, carrying out phishing campaigns, and extensive BEC scams, following a joint INTERPOL, Group-IB, and Nigerian Police Forcecybercrime investigation." The individuals are accused of creating phishing websites, domains, and mass-mailing operations in which they impersonated organization representatives. These ads were then used to spread 26 malware programs, spyware, and remote access tools, including AgentTesla, Loki, Azorult, Spartan, and the Nanocore and Remcos Remote Access Trojans. These applications were used to enter and monitor target organizations' and individuals' systems before conducting frauds and siphoning cash" (Interpol).

5.1.5 Economic, Social, And Political Impact of Addressing Cybercrime and Improving Online Safety, Emphasizing the Benefits of a Secure Digital Ecosystem for Africa's

Sustainable Development.

Combating cybercrime and increasing online safety may have enormous economic, social, and political impacts, especially in the context of Africa's long-term growth. Here are some of the possible benefits of a safe digital environment for Africa:

1. **Economic Development:** Trust and confidence in online transactions, e-commerce, and digital services are enhanced by a secure digital environment. It promotes more people andcompanies to participate in the digital economy, which results in greater economic activity,job creation, and innovation. This has the potential to contribute to Africa's overall economic growth and development.
2. **Foreign Direct Investment:** A safe digital environment draws international investors looking to set up shop or invest in Africa's expanding digital market. Improved cybersecurity and internet safety provide investors confidence that their investments will be safe, encouraging foreign direct investment (FDI) inflows into the continent. This can help to boost economic growth and development.
3. **Digital Inclusion:** By eliminating cybercrime and improving online safety, more people, particularly underprivileged groups, can participate in the digital revolution. Access to more secure digital platforms and services allows for increased engagement in e- commerce, online education, healthcare, and government services. This fosters social inclusion, bridges the digital gap, and provides new possibilities and resources to communities.
4. **Enhanced Governance and Digital Services**: Strengthening cybersecurity measures protects key infrastructure, government networks, and public services by ensuring the integrity and confidentiality of digital information. It helps governments to create safe online venues for citizen interaction, efficient service delivery, and open government. Thisbuilds confidence between residents and the government, resulting in greater accountability and more effective public administration.
5. **Personal Data Protection:** Addressing cybercrime helps to safeguard individuals' data and privacy. Strong data security standards and online safety safeguards secure sensitive information, allowing consumers to engage in online activities without fear of identity theftor data breaches. This encourages people to use digital services, resulting in a robust digitaleconomy. Building a safe digital environment demands regional and worldwide collaboration. African countries may collaborate to create common cybersecurity frameworks, discuss best practices, and share expertise about countering cyber threats. This engagement builds regional linkages, encourages knowledge transfer, and fosters creativity, eventually contributing to Africa's long-term prosperity.
6. **Enhanced National Security:** Cybersecurity is inextricably related to national security. African nations may protect themselves from cyberattacks, cyber espionage, and other online risks by investing in cybersecurity skills and increasing online safety. This improvesthe continent's overall security posture and provides the stability required for long-term growth.

Thus, combating cybercrime and enhancing online safety in Africa can have far-reaching economic, social, and political consequences. A secure digital ecosystem boosts economic growth,attracts foreign investment, promotes digital inclusiveness, improves governance, safeguards personal data, develops cooperation, and enhances national security. African states can harness thefull potential of the digital economy and set the route for long-term prosperity by emphasizing cybersecurity.

5.1.6 Artificial Intelligence, Machine Learning, And Blockchain Technologies Show Tremendous Possibilities for Strengthening Digital Defenses and Deterring Cybercriminal Activities.

Here's How Each of These Technologies Can Contribute to Enhancing Online Safety:

5.1.6.1 Artificial Intelligence (AI)

AI can improve digital security by analyzing massive volumes of data in real-time, identifying trends, and detecting abnormalities. Here are some examples of how AI might improve cybersecurity:

1. **Threat Detection and Prevention:** To identify possible dangers, AI algorithms can examine network traffic, user activity, and system records. By learning from trends and abnormalities, it can identify both known malware signatures and new varieties of malware.
2. **Advanced Threat Intelligence:** Threat intelligence systems driven by AI can continuallymonitor the global threat environment, gathering and analyzing data from numerous sources to identify new risks. This allows for proactive protection measures and quick responses to emerging cyber threats.
3. **User Authentication and Access Control:** AI can improve identification by using facialrecognition, voice recognition, and behavioural biometrics. It detects and prevents illegal access attempts, lowering the risk of account compromise and identity theft.

5.1.6.2 Machine Learning

Machine learning algorithms may learn from prior data, adapt to new risks, and improve over time.Here's how machine learning helps with cyber defence:

1. **Anomaly Detection:** Machine Learning models may detect out-of-the-ordinary patterns orbehaviours that differ from regular network activity. This algorithm can identify novel assaults and adapt to evolving dangers by continually learning from data, enabling early warning systems.**Malware Detection:** Machine Learning methods such as supervised and unsupervised learning may be used to identify and detect malware using source code, network traffic, orsystem performance. The models can detect malicious software even when it tries to avoiddetection by traditional signature-based approaches.
2. **Predictive Analytics:** Machine Learning algorithms can forecast future cyber threats by analyzing previous attack data, user behaviour, and system weaknesses. Organizations canproactively take security measures to prevent risks by identifying possible weak areas.

5.1.6.3 Blockchain Technology

Blockchain, having been a decentralized and transparent architecture, improves cybersecurity in the following ways:

1. **Secure Data Storage:** The decentralized nature of blockchain and cryptography protocolsassures data integrity and safety. Blockchain decreases the risk of data breaches and unauthorized alterations by storing sensitive information in a tamper-proof and irreversiblemanner.
2. **Digital Identity Management:** Blockchain can let individuals control their personal information by facilitating secure digital identities. It reduces the danger of identity theft and fraud by eliminating the requirement for centralized identity repositories.
3. **Smart Contracts and Secure Transactions:** The smart contract capabilities of blockchainenable safe and automated transactions. Blockchain decreases the danger of fraudulent operations and assures transaction integrity by removing mediators.
4. **Supply Chain Security:** By providing an auditable and transparent record of every transaction, blockchain can improve supply chain security. It allows for traceability, whichreduces the danger of counterfeit items, tampering, and illegal alterations.

Organizations may improve their ability to identify, avoid, and respond to cyber-attacks by utilizing the capabilities of Artificial Intelligence, Machine Learning, and blockchain technology.These technologies offer powerful analytical capabilities, real-time monitoring, and security frameworks that strengthen digital defences and prevent cybercriminal activity, resulting in a saferand more resilient online environment.

5.2 Online Safety: Measures and Solutions to Cybercrime

Online safety is necessary and validated as many businesses have been faced with excesses of attacks on the internet which has resulted in losing one’s life on the part of the victims, committingsuicide, or psychological disorderliness. Cyberattacks on business organizations are becoming a growing trend, and Africa is not exempted. The productivity, income, and client trust of organizations are all negatively impacted, not to mention the customers' security. For instance,

147.9 million individuals may have been compromised by the 2017 Equifax data breach hack. 150nations were affected by the May 2017 sad terror assault, including several in Africa. Companiesmust create a comprehensive strategy to safeguard their information assets and improve cybersecurity as this trend continues to grow to be ready to handle these cyber hazards (Equifax, 2017)

5.2.1 Push to Create and Implement’ Cyber Resilience Strategies

Considering the risk is constant and ever-growing, businesses must get ready for cyberattacks andbecome cyber-resilient. By prioritizing and implementing policies that will safeguard important assets and by incorporating them as requirements into all business activities, the board or executivelevel of the organization should start the process of building cyber resilience. Security ought to aidin the expansion of the company as envisioned by its long-term plan. Additionally, the business should strengthen its cyber capabilities by educating staff members about information security, formulating their information security skills, securing the configurations of its infrastructure and systems as a whole regularly updating those systems, utilizing technologies for active surveillance,putting proactive detection and rapid response to security breaches and incidents in place,conducting routine security audits, and performing penetration testing.

5.2.2 Improve, Strengthen, and Develop Cybersecurity Abilities

Online Safety and cybersecurity experience and qualified profiles are crucial to assist the cybersecurity menace but are relatively rare on the continent. Companies now need to create retention and skill-building plans to draw in and keep bright personnel who can help them implement their cyber security resilience. Because of the growing need for information security and cybersecurity experts globally, this will provide a unique challenge for organizations in Africa.In fact, from less than 1% in 2017 to 20% by 2020, experimental recruitment and talent retentiontechniques will be used in security skill management initiatives.

5.2.3 Safeguarding Data Integrity and Privacy

Data integrity may replace secrecy as the main criterion for cybersecurity. The revival of attacks,such as the several ransomware incidents that occurred in 2017 that were intended at modifying orerasing data, has brought attention to the significance of data integrity and the effects of data breaches on companies and individuals. Businesses must improve their security protocols to avoiddata corruption incidents and recover from them. Traditional methods, such as backups and routine system restoration, are crucial measures for this aim. Additionally, cutting-edge technologies likeblockchain may help to safeguard data integrity if businesses can minimize the negative risks as the technology is still in its early stages. Nevertheless, several African businesses, particularly in North Africa, have already begun to invest in new technologies to combat security risks. Information security contributions in the Middle East and North Africa increased by 11% in 2017to further expand to $1.8 billion. (Gartner Security and Risk Management Summit, 2017)

5.2.4 Initiate and Encourage Feasibility Studies (Assessment) of Cyber Threats in theDecision-Making Process

Relaying the dangers to all tiers of the decision-making system is the greatest strategy to involve senior management in the battle against cybercrime. This approach entails coordinating cybersecurity goals with the organization's strategic goals and identifying the vital assets and systems that should be protected as a matter of priority. To spread cyber risk-aware culture (raiseknowledge of the significance of preventing and solving cyber risks) at all levels of the firm, the objectives so stated can be properly financed and broken down at the tactical and operational levels.

6. Recommendations

In this digital age, information communications technology has assimilated into our everyday livesand cannot be done without it. Even though technology offers many benefits, it has also started toendanger our lives. It grew essential to use caution when utilizing any digital device to avoid fallingvictim to Cybercrimes. The following measures need to be carefully analyzed, implemented, and evaluated for a digitally safe online environment.

1. Feasibility studies and research to be conducted on the part of the Government onCybersecurity from time to time basics.
2. There should be minimal regulation on how the internet should be assessed especially for young people.
3. Cybersecurity education should be introduced into the educational sector for propersensitization and orientation from the grassroots.
4. Individuals shouldn't hide the perpetrators of these illegal activities in disguise on such accounts of the same people.
5. There should be a lengthened punishable offence for whosoever is found guilty of any stated cybercrime.
6. Appointment of under-covered secret agent(s) should be present in every community, company, school, and Governmental agency to monitor and report any form of malicious activities happenings around them.

Cybercrime shouldn't be handled with a minor task, a strong intelligent strategy should be put inplace to tackle the various insurgencies of crimes in the provision of advanced Technological Equipment, Professional expertise, a Fully funded research laboratory,

6.1 Suggestions: Government Approach to Cybercrimes and Online Safety

The continued progress of Africa in its effort to reach important digitalization heights is threatenedby the hazards and risks offered by cybercrime and its related activities. Although great efforts have been made, drastic and deliberate steps must be implemented to end this growing problem. When unequivocal facts and numbers are showing the enormous sums of finances that African nations are losing as a result of lenient laws that have allowed cybercrime to flourish, cybersecurity and cybercrime cannot be handled like every other subjected law. Governments need to formulatestrategies and policies that are successful in addressing the new security challenges related tothe illegal exploitation of Internet users.

1. **National Policy**

Joint and collaborative measures with stakeholders in cyber industries have to develop a nationalcyber security policy that recognizes the importance of critical information infrastructures and is capable of solving the cyber risks facing the countries as well as outline how objectives of suchpolicies can be achieved.

2. **National Strategy**

The adoption of careful and appropriate national strategies for fighting cybercrime is paramount. African Countries must implement effective national cyber security policies, particularly in the area of legislative reform, development, sensitization and capacity–building, public-private partnership, and international cooperation among others to achieve the needed results of sanitizingthe cyber society.

3. **Legislation Against Cybercrime**

Effective and efficient legislative and regulatory measures against cybercrime must be enforced by African countries. Clear and substantive criminal offences that affect the confidentiality, integrity, availability, and survival of information and communication technology must be encapsulated in legislative instruments.

4. **National Regulatory Authorities**

Governments as a matter of urgency should confer specific responsibilities on institutions and agencies, either newly established or pre-existing, as well as on the designated officials of the saidinstitutions, to confer on them an authority and legal capacity to act in all aspects of cyber securityissues, including but not limited to responding to cyber security incidents, and coordination and cooperation in the field of forensic investigations, prosecution, and enforcing cyber laws etc. There should be the promotion of technical education and the education of information and communication technology professionals, within and outside government bodies in the area of cyber security and cybercrime protection.

5. **Harmonization**

African countries should develop collaborative and harmonized efforts toward the fight against cybercrime. such efforts should be woven towards strengthening the possibility of regional harmonization of these measures and strategies. This by far will protect the region in a very broaderperspective rather than individual countries taking approaches that are not connected to the generalstrategy of the continent.

6.2 Cybercrime Safety Tips

Internet-enabled crimes and cyber intrusions are becoming increasingly sophisticated and preventing them requires each user of a connected device to be aware and on guard. National. (NCIJTF, Federal Bureau of Investigation)

1. Keep systems and software up to date and install a strong, reputable anti-virus program.
2. Be careful when connecting to a public Wi-Fi network and do not conduct any sensitivetransactions, including purchases, when on a public network.
3. Create a strong and unique passphrase for each online account and change thosepassphrases regularly.
4. Set up multi-factor authentication on all accounts that allow it.
5. Examine the email address in all correspondence and scrutinize website URLs beforeresponding to a message or visiting a site
6. Don’t click on anything in unsolicited emails or text messages.
7. Be cautious about the information you share on online profiles and social media accounts. Sharing things like pet names, schools, and family members can give scammers the hints they need to guess your passwords or the answers to your account security questions.
8. Don't send payments to unknown people or organizations that are seeking monetary support and urge immediate action.

7. Conclusion

Cybercrimes have caused more harm than good to all sorts of human society and full urgency hasto be dedicated both by Governments, Businesses, and individuals to point out these perpetrators to justice indulging in these illegal activities. Cybercriminals are getting more opportunities to perpetrate cybercrime as communication and information technologies progress. Cybercriminals are technically skilled professionals who employ a variety of techniques to compromise the privacy of people or organizations. Since anybody may become a victim of cybercrime and it can cause anindividual or an organization to incur losses in a matter of seconds, protecting against it is of utmostpriority. High measures of cybersecurity basic knowledge should be introduced in the educational curriculum for both young and adults to gain a wide range of knowledge. To determine the best solutions to secure sensitive data and take necessary precautions against cyber-attacks, a researchstudy of cybercrimes is required.

8. REFERENCES

Accenture, Insight Into The Cyber Threat landscape in South Africa, 2020. Available at: [https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-SouthAfrica-V5.pdf]

Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41. IGIGlobal, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001.

Amber Stabek, Paul Watters, and Robert Layton . (2010). The Seven Scam Types: Mapping the Terrain of Cybercrime. Second Cybercrime and Trustworthy Computing Workshop (pp. 41-51). Ballarat, VIC: IEEE.

Broadhurst, R G and Chantler, A. (2006) 'Cybercrime Update: Trends and Developments', In Expert Group Meeting on The Development of Virtual Forum against Cybercrime Report, June 28-30, 2006, Seoul Korea, KICJP & UNODC, pp. 21-56.

Bhanu Sahu, Neeraj Sahu, Swatantra Kumar sahu, and Priya Sahu. (2013). Identify Uncertainty ofCyber Crime and Cyber Laws. International Conference on Communication Systems and NetworkTechnologies (pp. 450 - 452). Gwalior: IEEE.

Bashir, Adil & Shoukat, Saba. (2018). Cyber Crime-Techniques, Prevention and Cyber Insurance.International Journal of Computing and Network Technology. 6. 23-26.

Dilek, Selma & Çakır, Hüseyin & Aydın, Mustafa. (2015). Applications of Artificial IntelligenceTechniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications. 6. 10.5121/ijaia.2015.6102.

Interpol, Interpol report shows an alarming rate of cyberattacks during COVID-19, 4 August 2020.Available at: [https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report- shows-alarming-rate-ofcyberattacks-during-COVID-19]

Institute for Security Studies, Africa can’t risk a major maritime cyberattack, Reva, D., 28 October2020. Available at: [https://issAfrica.org/iss-today/Africa-cant-risk-a-major-maritime-cyberattack]

Khan ER (1999). Developing the Theoretical and Conceptual Framework. Retrieved from: https:// journclasses.pbworks.comf/theoretical+framewor.ppt.

Kumar, Satish & Lim, Weng Marc & Sivarajah, Uthayasankar & Kaur, Jaspreet. (2022). ArtificialIntelligence and Blockchain Integration in Business: Trends from a Bibliometric-Content Analysis. Information Systems Frontiers. 25. 10.1007/s10796-022-10279-0.

McQuade S (1998). Towards a theory of technology-enabled crime. Unpublished manuscript. George Mason University, Fairfax, Virginia.

McQuade S (2006). Understanding and Managing Cybercrime, Boston:Allyn & Bacon.

USAID.GOV Cyber Crime: Its Impact on Government, Society and the Prosecutor An Aid for Assisting the Prosecutor in the Investigation, Trial and Conviction of the Cyber/Computer Criminal-https://pdf.usaid.gov/pdf_docs/Pnada641.pdf

Yassine, Maleh & Baddi, Youssef & Alazab, Mamoun & Tawalbeh, Loai & Romdhani, Imed. (2021). Artificial Intelligence and Blockchain for Future Cybersecurity Applications. 10.1007/978-3-030-74575-2.

Other Online Web Sources

Statista -https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/ Britannica -

https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy

Brookings -https://www.brookings.edu/articles/cybersecurity-in-africa-securing-businesses-with-a-local-approach-with-global-standards/

Equifax Breach Settlement -https://www.equifaxbreachsettlement.com/ Federal Bureau of Investigation -

https://www.fbi.gov/investigate/cyber Learning - https://www.learning.com/blog/online-safety-definition-

basics/Merriam-Webster - https://www.merriam-webster.com/dictionary/Internet

Mustard Insights -https://blog.mustardinsights.com/in-africa/african-countries-with-the-most- phishing-attacks-2022-paD8h

Wikipedia - https://en.wikipedia.org/wiki