Sub-Sahara African Academic Research Publications
March, 2023 Editions

JHSPR
Journal of Human, Social & Political Science Research.
Vol.27, No.6, ISSN:2416-7999

DEVELOPING NEW LEGAL APPROACHES TO ADDRESS CYBERSECURITY CHALLENGES IN AFRICA.

LATEEFAT ADEOLA BELLO Ph.D
Department of Commercial Law, Faculty of Law, Ahmadu Bello University, Zaria

ABSTRACT

Cybersecurity refers to the practice of protecting computers, networks, and digital information from unauthorized access, theft, damage, or other forms of cyberattacks The rise of cybersecurity threats in Africa has become a major concern for governments, businesses, and individuals. Traditional legal frameworks often struggle to keep up with the rapidly evolving nature of cyber threats, and as a result, many countries in Africa have been struggling to address this issue effectively. Interestingly, The continent has no unified approach to tackling cybercrime, and this constitutes a hindrance to enacting and enforcing effective laws and regulations. This lack of regulation leaves African countries vulnerable to a wide range of cyber threats, including data breaches, internet fraud, and online scams. This paper explores the challenges of addressing cybersecurity threats in Africa and proposes new legal approaches to include developing comprehensive cybersecurity laws that take into account the unique challenges faced by African countries, strengthening regional cooperation and coordination in combating cybercrime, increasing public awareness about cybersecurity risks and best practices, and promoting the development of a robust cybersecurity industry. The paper further highlights the importance of building the capacity of African countries to address cybersecurity challenges, particularly in terms of building the technical skills of law enforcement agencies, judges, and prosecutors. It emphasizes the need for collaboration between governments, the private sector, and civil society in addressing the issue of cybersecurity in Africa. The paper adopts the doctrinal approach in the discourse on the importance of developing new legal approaches to address cybersecurity challenges, protecting critical infrastructure, promoting economic growth and development, and ensuring the safety of electronic transactions and activities across the African continent.

Introduction

Cybersecurity is the practice of protecting computers, networks, and digital information from unauthorized access, theft, damage, or other forms of cyberattacks. Preventing and mitigating cyber risks, which might include viruses, malware, phishing, hacking, and other nefarious actions, involves a set of policies, procedures, and technologies. Protecting data and information systems from illegal access, use, disclosure, disruption, alteration, or destruction is the main objective of cybersecurity. Firewalls, antivirus software, intrusion detection systems, encryption, multi-factor authentication, and other safeguards against online attacks are examples of cybersecurity measures. Sub-Saharan African banks are particularly susceptible to cyberattacks, according to Dataprotect, a data security firm with headquarters in Morocco. This is mostly because of a shortage of experienced experts and a lack of investment in cybersecurity. His survey's findings published in 2020 revealed that more than 85% of the twenty-one (21) banks from West Africa to Central Africa had already been the target of at least one cyberattack. A third of these attacks used phishing, while over 30% involved bank card fraud (Jason Mitchell).

Internet usage is increasing significantly in African countries as more businesses adopt the practice of e-commerce and regular consumers start utilizing the same without being aware of the risks as technology continues to evolve quickly and become more integrated into daily life. These nations thus have the greatest number of cybercrime victims worldwide (Okelo-Odongo B. and . McConnell, S, 2018) As a result, cybersecurity has emerged as a crucial concern for people, companies, and governments all around the world. Due to the recent increase in cybercrime and hacking attacks, both private and public organisations have suffered considerable financial losses, privacy violations, and reputational harm. According to a report from the cybersecurity consulting company Serianu, cybercrime cost Africa $2.2 billion in losses in 2019 and is expected to cost $5.6 billion by 2025 (Serianu, 2020)[3]. Both the city administration of Johannesburg and the National Security Agency of Nigeria have experienced assaults that have disrupted operations or exposed private information. Experts are concerned that cyberattacks targeting marine infrastructure, such as privacy database logs, might seriously impair Africa's ports and shipping industry. Both public and private organizations, such as governmental organizations, financial institutions, and telecommunication corporations, have been impacted by these cybersecurity issues. Phishing, spyware, ransomware, and distributed denial-of-service (DDoS) attacks are the most typical cyberattacks in Africa. Cybercriminals frequently carry out these attacks to steal confidential data, demand ransom, or damage vital

infrastructure. Since foreign governments and state-sponsored organizations attack their political and military institutions, many African nations also struggle with issues connected to cyber espionage and cyber warfare (Okelo-Odongo. B and McConnell, S, 2018).

The absence of a thorough and cohesive cybersecurity strategy in Africa has made it simpler for cybercriminals to operate internationally and take advantage of weaknesses in current legal systems. Numerous African nations have passed rules and regulations intended to safeguard their residents and businesses from cybercrime, but they have mainly proven ineffective at fending off online dangers. This is caused by several things, such as scarce resources, ineffective institutions, and low public knowledge of cybersecurity. In addition, the COVID-19 epidemic As more individuals work from home and rely on digital technologies for communication and commerce, cybersecurity concerns in Africa are getting worse. The rising reliance on digital platforms has given hackers new opportunities to launch new types of assaults, like phishing schemes based on COVID-19. Strengthening the legal frameworks is one way to address the specific issues African countries confront to combat these challenges, which call for a comprehensive and coordinated strategy. (African Union Convention on Cyber Security and Personal Data Protection, 2014).

Current cybersecurity legal framework in Africa

Significantly, Africa's present legal system for cybersecurity is disjointed. Most nations do not have thorough legal systems that cover every facet of cybersecurity and offer a framework for inter-African collaboration and information exchange. Yet, several noteworthy initiatives are starting to emerge to create the necessary legal frameworks and enhance cybersecurity in Africa The Convention on Cyber Security and Personal Data Protection, which was adopted in 2014, was created with leadership from the African Union (AU). The Agreement offers African nations a legal framework to combat cybercrime and safeguard personal data. The Agreement also creates a framework for information sharing and cooperation among African nations, which is essential for solving cybersecurity issues[6]. Some African nations have passed cybersecurity legislation and regulations in addition to the AU Convention. For instance, the Cybercrimes and Cybersecurity Bill was passed in South Africa (Cybercrimes and Cybersecurity Bill, South Africa, 2017) This makes cybercrimes illegal and creates a structure for stopping and looking into them. The Cybercrimes (Prohibition, Prevention, etc.) Act (Cybercrimes (Prohibition, Prevention, etc.) was also passed in Nigeria which makes cybercrimes illegal and

enables police to look into and prosecute offenders. In addition to developing a National Cybersecurity Policy and Strategy that offers a framework for addressing cybersecurity issues, some African nations like Kenya also produced a National Cybersecurity Strategy and Implementation Plan (Tonui,P. & Oboko, R.K pp. 148-157) Notwithstanding these initiatives, the majority of African nations still lack suitable legal frameworks to manage the complex and dynamic nature of cyber threats. The actions listed below can improve Africa's cybersecurity capacities and encourage a safer and more secure digital environment:

1. Creation of comprehensive cybersecurity laws and regulations: African nations can create comprehensive cybersecurity laws and regulations that address all aspects of cybersecurity, including the criminalization of cybercrime, the protection of personal data, and the creation of a framework for cooperation and information sharing among African nations.
2. Ratification and implementation of the AU Convention on Cyber Security and Personal Data Protection: The Convention on Cyber Security and Personal Data Protection, which offers African countries a legal framework to combat cybercrime and protect personal data, is ratifiable and implementable by African countries.
3. A framework for collaboration and information exchange between African nations should be established by the Convention. 2 Creation of cybersecurity agencies: To plan and direct cybersecurity operations, African nations may create cybersecurity organizations. These organizations can act as hubs for information exchange and cooperation among African nations.
4. Establishing partnerships and collaborations: To improve their cybersecurity capabilities, African nations can establish partnerships and collaborations with other nations, international organizations, and the private sector. These collaborations can make it easier to share information and work together on cybersecurity challenges.
5. Investment in capacity-building and awareness-raising programs: To improve their cybersecurity capabilities, African nations can make investments in capacity-building and awareness-raising initiatives. These initiatives may involve public awareness campaigns as well as training for the judiciary, law enforcement, and other stakeholders. African nations can promote regional and continental collaboration on cybersecurity-

related challenges. These frameworks can make collaboration and information-sharing on cybersecurity challenges easier.

Many African nations have passed laws and regulations intended to safeguard their citizens and businesses from cybercrime, but they have largely proven ineffective at fending off online dangers. Because there isn't a comprehensive, unified approach to cybersecurity, it is simpler for cybercriminals to operate internationally and take advantage of gaps in the system's existing legal systems. Therefore, it is imperative to create fresh legal strategies to handle Africa's cybersecurity issues. The strategies should be conscious of the particular difficulties faced by African nations, such as few resources, frail institutions, and low public knowledge of cybersecurity. Along with being adaptive to the continuously changing nature of cyber threats, legal strategies should also be able to keep up with new and developing trends. Furthermore, legal strategies should be flexible enough to accommodate the continuously changing nature of cyber risks and be able to keep up with new and developing patterns in cybercrime. It is imperative to create new legal strategies to handle cybersecurity issues in Africa for several reasons, some of which are outlined below: which is;

Legal approaches should also be adaptable enough to take into account the constantly shifting nature of cyber hazards and be able to keep up with emerging trends in cybercrime. For several reasons, some of which are listed below, new legal approaches to tackle cybersecurity challenges in Africa are essential(Achilleos, A. 2018 pp. 221-240.) Second, cybersecurity is essential for Africa's economic development and progress. Threats to cyber security can result in large financial losses, which can have a severe effect on enterprises and the economy as a whole. Creating new legislative frameworks that defend people and organizations from cyber threats can contribute to the improvement of the security and stability of the environment for financial investment and economic development (Tonui and R. . Oboko, K pp. 148-157, 2016). Thirdly, cybersecurity is essential for protecting the privacy and security of citizens. As more people rely on digital technologies for communication, commerce, and personal information storage, there is a growing need for legal frameworks that protect citizens' rights to privacy and personal security.

(Emecheta . C pp. 2020 pp.32-45)

Lastly, cybersecurity is critical for national security and stability. Cyber-attacks on critical infrastructure, such as power grids, water systems, and transportation networks, can have severe consequences and disrupt social and economic activities. Developing new legal approaches to address cybersecurity challenges

can help to prevent such attacks and protect national security and this requires a comprehensive and coordinated approach that involves all stakeholders, including governments, the private sector, and civil society (Tonui and R. . Oboko, K pp. 148-157, 2016)

Other important reasons why developing new legal approaches to address Africa's cybersecurity challenges is critical.

The general public's lack of cybersecurity awareness is one of the most significant challenges confronting African countries. Many people are unaware of the dangers of digital technologies or how to protect themselves from cyber threats. As a result, they are more vulnerable to cyber-attacks, creating an environment in which cybercriminals can easily exploit vulnerabilities. Creating new legal approaches to promote cybersecurity awareness and education and education can help to raise public awareness and encourage people to take proactive measures to protect themselves(Kimathi E.H and Njoroge, N.N 2019 pp. 54-65)[7] Another important reason for developing new legal approaches is to address the continent's lack of cooperation and coordination. Cyber threats have no regard for borders, so addressing these challenges effectively requires a regional approach. African countries can work together to combat cyber threats by developing new legal frameworks that promote regional cooperation and information-sharing, which can help to strengthen cybersecurity across the continent (African Union Convention on Cyber Security and Personal Data Protection, 2014) Finally, developing new legal approaches to address cybersecurity challenges can aid in bridging Africa's digital divide, as most African countries face significant challenges in terms of digital inclusion, resulting in a digital divide that limits access to digital technologies and opportunities. These countries can promote cybersecurity to create a more secure and stable environment that encourages investment in digital technologies and bridge the digital divide to promote economic development. (United Nations General Assembly Resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security," 2015). These policy and regulatory solutions can be implemented to improve cybersecurity in Africa.

What are the limitations of existing legal frameworks?

Although some regulatory frameworks are in place to address cybersecurity issues in Africa, several constraints must be addressed. These are some of the restrictions: The lack of legal framework harmonization among African nations makes it more difficult to coordinate cross-border responses to cyber threats, reducing the effectiveness of regional and global collaboration. Similarly, some African countries' legal systems lack effective enforcement mechanisms. This suggests that even when cyber crimes are discovered, they may not be

thoroughly investigated and prosecuted. It has also been noted that some legislative systems do not adequately protect critical information infrastructure, such as financial systems, communication networks, and power grids. Their vulnerability to cyberattacks is extremely high which can increase security risk. Other reasons may include:

a. Inadequate capacity: Many African countries lack the technical expertise and financial resources required to implement and enforce comprehensive cybersecurity legal frameworks. This means they may be ill-equipped to respond to cyber threats effectively.
b. Lack of public awareness: There is a lack of public awareness of the importance of cybersecurity in Africa. This means that individuals and organizations may fail to take adequate cyber-security precautions. (World Bank Group. (2016)

To address these limitations, African countries must develop more comprehensive cybersecurity legal frameworks that account for the evolving nature of cyber threats. This should be done in collaboration with regional and international organizations to ensure cross-border harmonization and effective coordination of cyber threat responses. There is also a need to invest in increasing the capacity of law enforcement agencies and other stakeholders to respond to cyber threats effectively. Finally, increased public awareness of the importance of cybersecurity and how individuals and organizations can protect themselves from cyber threats is required. (United Nations Office on Drugs and Crime. (2013)

Furthermore, developing comprehensive cybersecurity laws in African countries necessitates a multi-pronged approach that includes conducting a cybersecurity assessment, establishing a legal and regulatory framework, developing a cybersecurity strategy, capacity building, forming partnerships, and ensuring public participation. These steps can assist in ensuring that the legal frameworks in place are effective and responsive to the changing nature of cyber threats. (African Union Convention on Cyber Security and Personal Data Protection2014) Countries can also establish regional cybercrime centres that will be in charge of dealing with cybercrime in the region. These centres can share information, coordinate investigations, and provide technical assistance to member countries. Ratification of international cybersecurity treaties and conventions: African countries can ratify international cybersecurity treaties and conventions, such as the Budapest Convention on Cybercrime, which provides a framework for international cybercrime cooperation. African countries can strengthen their ability to cooperate and collaborate with other countries in combating cybercrime by ratifying these conventions.

Countries can also establish regional cybercrime centres to handle cybercrime in their respective regions. These centres can share information, coordinate investigations, and offer member countries technical assistance. Ratification of international cybersecurity treaties and conventions: African countries have the option of ratifying international cybersecurity treaties and conventions such as the Budapest Convention on Cybercrime, which provides a framework for international cybercrime cooperation. By ratifying these conventions, African countries can strengthen their ability to cooperate and collaborate with other countries in combating cybercrime.

Countries can also conduct joint training and capacity-building programs to improve their technical expertise and financial resources in combating cybercrime. more efficiently. This includes enacting laws that criminalize cybercrime and provide for effective cybercrime investigation, prosecution, and punishment, as well as ratifying international cybersecurity treaties and collaborating on training. One example is sharing information on successful investigations, prosecutions, and other counter-cybercrime measures. African countries can strengthen their legal frameworks to combat cybercrime more effectively through joint training and capacity-building programs, sharing best practices, and strengthening legal frameworks. Sharing information on successful investigations, prosecutions, and other measures that have been effective in combating cybercrime is one of the measures that can help the region's ability to prevent, detect, and respond to cyber threats. include sharing information on successful investigations, prosecutions, and other measures that have been effective in combating cybercrime. These measures can help to enhance their ability to prevent, detect, and respond to cyber threats in the region. include sharing information on successful investigations, prosecutions, and other measures that have been effective in combating cybercrime. African countries can strengthen their legal frameworks to ensure they effectively combat cybercrimes (United Nations Office on Drugs and Crime. (2020). These measures can help to enhance their ability to prevent, detect, and respond to cyber threats in the region (Miti, M. C., & Kilic, H. (2019) 221-234). To summarize, raising public awareness about cybersecurity risks and best practices is critical for safeguarding individuals, organizations, and critical infrastructure against cyber threats. African countries can raise public awareness through the development of cybersecurity awareness programs, cybersecurity training and education, media campaigns, collaboration with the private sector, and the development of national cybersecurity policies(SANS Institute. (2018). These measures can aid in the development of a cybersecurity culture and ensure that individuals and organizations are better prepared to respond to cyber threats.

Promoting the development of a robust cybersecurity industry

Promoting the development of a robust cybersecurity industry is crucial for addressing cybersecurity challenges in Africa. African countries can encourage

investment in the cybersecurity industry by creating a favourable investment climate, such as providing tax incentives and other benefits to cybersecurity companies. Governments can also partner with the private sector to provide funding and other resources for cybersecurity startups. African countries can also support research and development in the cybersecurity industry by providing funding for research projects and academic programs that focus on cybersecurity. This can help to foster innovation and the development of new cybersecurity technologies. In summary, building the capacity to address cybersecurity challenges is essential for ensuring that African countries have the skills and resources needed to address cyber threats. African countries can build capacity by developing cybersecurity training programs, promoting cybersecurity research and innovation, enhancing public-private partnerships, establishing cybersecurity centres of excellence, and building cybersecurity workforce capacity. By taking these steps, African countries can build a strong foundation for addressing cybersecurity challenges and protecting their citizens and critical infrastructure from cyber threats World Economic Forum 2019). It is important to note that by adopting a multi-stakeholder approach to cybersecurity, African countries can create a more secure and resilient cyber environment that supports economic growth, development, and innovation. Ultimately, the success of cybersecurity legal approaches in Africa depends on the commitment and cooperation of all stakeholders. African governments, the private sector, and civil society must work together to develop and implement comprehensive and effective legal approaches that address the growing cybersecurity threats facing the continent. In addition. African countries can adopt international cybersecurity standards, such as the ISO 27001 and the NIST Cybersecurity Framework, to guide the development of their cybersecurity legal frameworks (World Economic Forum 2019). This will help ensure that their legal frameworks are aligned with global best practices and can facilitate international collaboration and information sharing. Establishment of cyber incident response teams: African countries can establish cyber incident response teams to respond to cyber-attacks and other cybersecurity incidents. These teams can be comprised of representatives from the government, the private sector, and civil society and can work together to prevent and mitigate cybersecurity incidents and integrate cybersecurity into education and training programs to build a culture of cybersecurity awareness and best practices. This can include cybersecurity awareness campaigns in schools, universities, and vocational training programs. African countries can also promote international collaboration and information sharing through participation in regional and international cybersecurity initiatives, such as the African Union Convention on Cyber Security and Personal Data Protection, the Commonwealth Cyber Declaration, and the Global Forum on Cyber Expertise (United Nations. (2020). Global Cybersecurity Index 2020)

In conclusion, the development of new legal approaches to address cybersecurity challenges in Africa is an urgent priority. African countries must take proactive measures to address the growing cybersecurity risks and threats facing the continent. The paper recommends that African countries adopt the identified measures to develop effective legal approaches that promote cybersecurity, innovation, and economic growth. They can also help establish a culture of cybersecurity that is essential for the development of a secure and resilient cyber environment in the best interest of Africa.

REFERENCES

Jason Mitchell, (2022) Africa faces huge Cybercrime Threat as the pace of digitalization Increases Investment Monitor. Available at https://www.investmentmonitor.ai/features/africa-cyber-crime-threat-digitalisation. Accessed 20 February 2023[1] 3 B. Okelo-Odongo and S. McConnell, "Cybersecurity in Africa: Risks, Challenges and Opportunities," Journal of Cyber Policy, vol. 3, no. 3, pp. 302-318, 2018.

B. Okelo-Odongo and S. McConnell, "Cybersecurity in Africa: Risks, Challenges and Opportunities," Journal of Cyber Policy, vol. 3, no. 3, pp. 302-318, 2018.3.

Tonui. P and Oboko, R.K "Cybersecurity in Africa: A Review of Current Challenges and Proposed Solutions," International Journal of Computer Science and Information Security, vol. 14, no. 10, pp. 148-157, 2016

Cybercrimes (Prohibition, Prevention, etc.) Act, Nigeria,

Cybercrimes and Cybersecurity Bill, South Africa, 2017.

Cybercrimes (Prohibition, Prevention, etc.) 2015.

(2020). Africa cybersecurity report 2020. Retrieved from https://www.serianu.com/wp-content/uploads/2020/09/Africa-Cyber-Security-Report-2020.pdf Retrieved 19 February 2023

African Union Convention on Cyber Security and Personal Data Protection, 2014.

B. Okelo-Odongo B. and . McConnell, S. "Cybersecurity in Africa: Risks, Challenges and Opportunities," Journal of Cyber Policy, vol. 3, no. 3, pp. 302-318, 2018.

African Union Convention on Cyber Security and Personal Data Protection, 2014

World Bank Group. (2016). Cybersecurity in East Africa: An Overview of the Policy and Legal Frameworks. Retrieved from https://www.worldbank.org/content/dam/Worldbank/document/fragility-conflict-and-violence/Cybersecurity%20in%20East%20Africa.pdf

United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime. Retrieved from fhttps://www.unodc.org/documents/cybercrime/Comprehensive_Study_on_Cybercrime.pdf

African Union Convention on Cyber Security and Personal Data Protection. (2014). African Union.

Achilleos A, 2018 "Legal Challenges of Cybersecurity in Africa," African Journal of Legal Studies, vol. 10, no. 2, pp. 221-240.

P. Tonui and R. . Oboko, K "Cybersecurity in Africa: A Review of Current Challenges and Proposed Solutions," International Journal of Computer Science and Information Security, vol. 14, no. 10, pp. 148-157, 2016.

United Nations Office on Drugs and Crime. (2020). Comprehensive Study on Cybercrime. Retrieved from https://www.unodc.org/documents/data-an analysis/statistics/crime/cybercrime/Comprehensive_Study_on_Cybercrime.pdf

Miti, M. C., & Kilic, H. (2019). Strengthening regional cooperation and coordination to combat cybercrime in Africa. African Journal of Science, Technology, Innovation and Development, 11(2), pp 221-234.

SANS Institute. (2018). State of Cybersecurity in Africa. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/state-cybersecurity-africa-38070

21. United Nations. (2020). Global Cybersecurity Index 2020

.United Nations. (2020). Global Cybersecurity Index 2020. Retrieved From Https://www.Itu.Int/Dms_Pub/Itu- D/Opb/Str/D-Str-Gci.01-2020-Pdf-E.Pdf