OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
11 - 18

Evidence-Based Critical Infrastructure Intelligence and Resilience Actions Against Cyber Cybersecurity Inequities

Ernest Tambo[1,2,5], Kennedy Okorie[1,3], Ngo Tappa Tappa[1,3,4] Narcisse Ngouamo[1,3], Hoberlin Fotsing Sadeu[1] , and Patience N Njinyah[1,3]
[1]Africa Disease Intelligence, Preparedness and Response, Yaoundé, Cameroon
[2]School of Public Health, Faculty of Medicine, Universite des Montagnes, Cameroon
[3]Department de Sante Publique, Faculté de Médecine, Université de Douala, Cameroon
[4]Association for Equity, Resilience and Wellbeing in Africa (APERA)
[5]Center for Leadership in Global Health Equity, University of Global Health Equity, Kigali, Rwanda
tambo0711@gmail.com

ARTICLE INFO

Article History
Received 25 Oct 2023
Received in revised form 31 Jan 2024
Accepted 27 Feb 2024

Keywords:
Cyber-defense, cyber-resilience, partnership, data sharing, vulnerability, cyberattacks

ABSTRACT

There is an emerging trend of cyber inequity between countries, corporates and organizations, evolving technological transition, current cyber-skills and workforce shortage that calls for an urgent needs and importance of building a better local and global cybersecurity ecosystem. The scale and sophistication of cyberattacks/threats and cybercrimes landscape continue to fuel the lucrative nature of ransomware, automation disruption, theft of intellectual property and data business concerns. There is urgent need to enhance cyber resilience and defense systems by prioritizing and investing in improving cyberdefence and cyber-resilience postures of governments and critical firms, as variety of complex systems and technologies are becoming increasingly vulnerable to attacks, incidents and threats/crimes. The article assesses critical infrastructure and population data vulnerabilities in shaping cyberdefence and cyber-wellness in targets domains against cyberthreats, attacks and cybercrime globally and in Africa particularly. We documented that increasing ransomware, extortion and ubiquitous phishing supply chain attacks are now all commonplaces. Our findings showed that financial services, mining and healthcare, travel and personal information and identity are the most affected domains. The most vulnerable African countries were namely Ethiopia, Nigeria, South Africa, Algeria, Rwanda and Kenya. Phishing was by far the most prevalent crime with growing prevalence of others. Scaling up cybersecurity and compliance solutions requires a coordinated and dedicated commitment and investment to cyberdefence in Africa. Proactive multisectorial partnership and data sharing collaboration is a potential game changer and resiliency to keep cyber-threats on surveillance check, priorities settings and aligned national actions plans. Sharping shared focus and bringing parties and stakeholders together is essential in building crucial evidence-based cyberdefence and cybersecurity, vulnerability monitoring and compliance solutions. Our results are discussed in improving data-driven or evidence-based cybersecurity intelligence, cyberdefence data sharing protection and improved public–private partnership those are essential building blocks in increased regulatory enforcement, legislative reforms actions and protection measures including digital trust, cyber-inclusive future and resiliency against cyberattacks vulnerabilities, losses and damages. Timely and continuous cyber information triage, analysis and shared cybersecurity and cyberdefence intelligence such as artificial intelligence and deep machine learning potential applications from multisource have immense potential to enrich more contextual and actionable defensive

ISSN 2636-9680
eISSN 2682-9266

capacities including threat detection and mitigation intelligence, cyber information equitable sharing, early waning and response systems.

I. INTRODUCTION

Hastening internet permeability coupled with COVID-19 infodemics has given rise to an upsurge in digital transformation across the globe. Cyberattacks are proliferating causing turmoil among organization in nations affecting health, financial and mining firms tempering with privacy integrity. Essentially, cyberattacks or threat could be seen as any form of un authorized entry or jeopardy of financial integrity, cessation of ongoing processes, or soiling to the eminence of an intuition as a results of a breakdown of its information technology (IT) systems, as spell out by the Institute of Risk Management (IRM) (1).

Cybersecurity involves the clustering of technologies, procedures and applications constructed to ensure integrity of information processing systems from intrinsic or extrinsic blackmail and unwarranted entrance(1,2).The Global Risk Report by the World Economic Forum, estimated squandered financial resources due to cyber threats is estimated as US$ 6 trillion as of 2021(3,4) . Digitalization of trade and business operations through the Internet of Things (IoT), Artificial intelligence (AI), cloud computing, mobile, block chain, and upcoming technological revolutions, cyber threat is ingrained and extremist (4). This section should provide the background on the context of the problem. Justify and rationalize the importance of the research. State the problem statement and the matters to be discovered and the steps the researcher took to fill the gaps or improvements to the situation such as the research objectives, scope, solutions and the contribution of the findings.

II. THE GROWING TREND OF CYBERATTACKS

Cyberattacks are a growing geopolitical risk, becoming larger, more intricate and more relentless. They are a significant threat to firms, organizations and national security. The United States of America is facing a widespread ransomware issue, and the US government is demanding stricter safeguards to help protect against such threats. The European Parliament website was made inaccessible for several hours in November 2022, with a pro-Kremlin group claiming responsibility for the cyberattack. Moldova's government suffered a data breach as recently as January 2023, and Australia's second-largest telecom company, Optus, suffered a data breach in September 2022 (1,4). The digitization of critical national infrastructure (CNI or health data) means that many essential services, including power grids, water supply networks and transportation systems, are increasingly vulnerable to cyberattacks. A successful cyberattack on any of these systems can have severe consequences, including loss of life and economic damage. The repercussions of persistent cyberattacks and cybercrimes could have a wide-reaching impact on financial markets and the economy. Government networks, private sector networks and infrastructure are all susceptible to hacking and espionage. International cooperation to effectively address cyberattacks is challenging given the complex geopolitical relationships between many countries, and climate-conflict linked poverty vicious cycle. As wars and geopolitical tensions rise between some of the world's major powers igniting critical and targeted structures and data cyberattacks vulnerabilities and corporate criminalities losses and damages (2,5)

The lack or inefficiency of cyberspace local and international laws enforcement against infringements resulted closely to $7 billion of financial loss, and about $15 million stored data were revealed through breaches 2021-2022, compared to over 300 businesses attacks since June 2022 to date in United States of America. For example, both Uganda telecoms and the Banking sector found themselves embedded in crisis due to hackers gaining access to Uganda money network services of which became more solicited as a result of COVID-19 pandemic. Nearly, estimated $3.2 million lost as results of hackers utilizing approximately 2000 Subscriber Identity Module Cards in establishing mobile money payment scheme. The subsequent largest

healthcare provider was targeted by a cyber-attack amidst COVID-19 pandemic, incapacitating 6500 private healthcare bed

provider, giving them no options than to revert to manual backup systems (5,6,7).

However, building evidence-based resilient and robust cyberdefence and cybersecurity partnership and data security guidelines to sharing intelligence against critical infrastructure cyberattacks and vulnerabilities summing up remain considerably low in African nations (2,3,5,6,7).. One of the most predominant puzzle regarding cyberdefence and cyber-wellness safety in policies and regulations are not adequately integrated across the board in Africa and worldwide. Cybersecurity requires continuous investment in an area where best practices are a moving target due to its evolutionary, adversarial and asymmetric nature and mostly scarcity of evidence research on cybersecurity leadership on market opportunities. Better understanding of competitive advantage and potential risk categories and factors for resilience building and strategic allocation of resources.

This article assesses shared cyber-attacks and crime vulnerabilities trends in harnessing evidence-based mutlisectorial/transnational cyberdefence/cybersecurity partnerships and data sharing intelligence and collaboration, comprehensive cyberdefence prevention and mitigation strategies implementation in targets critical infrastructure and populations in Africa and worldwide.

III. IMPLEMENTING CYBERSECURITY AND CYBERDEFENCE PARTNERSHIP, DATA SHARING POLICY AND GOVERNANCE FRAMEWORK

Our findings reported an increasing malware attacks, cybercrimes is now of a dynamically and recurrently threat surfacing out with new digital initiatives and a series of weaponry technological innovations in other to cause more disruption and damage to users of essential digital infrastructures at massive scale. There is a necessity in involving civil society in nationwide cyber security blueprint and policy more than ever. Civil society ensures proper dissemination of national cyber security strategies, so that it can be broadly read, popularly acknowledge, so that intuitions like state, private enterprises, and other actors are held liable for misconduct(11).Fostering collaboration with government, so as to permit the identification of susceptible sectors and facilitating in incident response and recovery solutions is of utmost importance in safeguarding essential national infrastructure(11).

These major cyber-attacks reported come in different forms, such as espionage attempts, Denial-of-Service (DoS) attacks and ransomware attacks. For Example, a cyberattack that disrupts hospital services can have serious consequences, such as delaying emergency care, cutting off supplies and services, or causing the death of patients. The increased digital device and network activities have attracted many hackers that seek to steal personal information or disrupt services. In addition, cybercriminals have also attempted to compromise hospitals and research centers on cybersecurity and cyberdefence research needs is substantial and not limited to professionals (12).

This requires public and private partnership and cyberspace collaboration and governance in other to boosting participative cybersecurity investment and promoting threat or crime information intelligence sharing, adhering to international cybersecurity principles, norms and best practices. Harnessing effective and efficient mitigation and adaptation methods to cyber-incidents response plans. In addition, strengthening evidence-based cyber maturity and reactiveness, in early real time, resilient and robust detection and response to threats or crimes. There is a need to create a cybersecurity ecosystem and platforms where global users of all ages need to be educated and be aware of the risks of the cyber world and must be prepared to fend off-hackers that attempt to infiltrate their networks and personal accounts. Mobile, digital and cloud-based-internet designers and users should avoid giving out personal information or opening doubtful websites and application software (13) (Table 1)

ISSN 2636-9680
eISSN 2682-9266

TABLE 1: Summary of cyberattacks and crimes across Africa and worldwide

Cybercrimes and attacks	**Key solutions and recommendations**
Non-payment and non-delivery	▪ Promotion of Public private partnership ▪ Building cross sectorial collaboration ▪ Enhanced data protection and data security ▪ Enhanced email and document encryption ▪ Fast tracking cyber resilience digital signing ▪ Proactivity and more efficient recovery tactics ▪ Computer biometric and cryptographic solutions ▪ Personal information protection on social media
Personal data breach	
Phishing, whaling and pharming	
Extortion	
Identity theft and password attack, email frauds, social media frauds	
Malware, ransomware, soyware, Trojans, deepfakes	
Denial of services and Tunneling	
Online scam and cryptocurrency	
Cyber espionage	
Clickjacking	
Banking frauds	
Trafficking	
Malacious email and website	
Major malware attacked by countries in 2022	**Percentage (%)**
Ethiopia	62%
Algeria	59%
Burundi	57%
Rwanda	46%
Kenya	41%
Nigeria	40%
Zimbabwe	40%
Ghana	39%
Zambia	38%
South Africa	36%
Uganda	36%

IV. STRENETHENING LOCAL AND REGIONAL CYBERDEFENCE AND CYBERSPACE CAPACITY BUILDING

Setting up the enabling law enforcement for law enforcement to proactively defend and counter cyber threats against law enforcement networks and critical technologies security, safety and protection environment including intellectual property rights (IPR) is essential for cybersecurity mobile and digital to Artificial intelligence services delivery, telecommunication and social media services, monitoring information system building capacity. Also, offer safety compliance support to companies and stakeholders in securing their infrastructure, transactions and online services, application and data confidentiality, with a wider range of solutions and technical assistance. The growing sophistication of cyber-threats and attacks require more preparation including capacity building and training for collective defense, crisis management and cooperative security, aligning with international laws, enhance local and regional resilience and provide a platform for advocacy and political consultation to collective action.

Cyber related crime lansdscape is likely to continue and evolve, from critical infrastructures and businesses email compromise, ransomware, data theft and extortion, impersonations, scams, phishing / smishing (including “quishing” through QR codes), credential stuffing and extortions globally. While health, financial services and retail are likely to remain key focus areas, we also see increased risk for our essential services / critical infrastructure. We are yet to see an attack that has a prolonged impact on the operational integrity of critical assets. This is perhaps one of our biggest risks, more serious in many respects than a cyber incident affecting data alone.

Although building and maintaining cyberattacks to cyberspace are complex, destructive and becoming ever more frequent,

continuous adaptation to the evolving threat an crime landscape require strengthening African countries cybersecurity and cyberdefence posture. Mauritius is usually quoted and advertence in the globe due to its cyber security capabilities , its judicial and functional infrastructure, its nationwide cyber security agency (CERT-MU), its national capacity building and cognizance leadership, and the implication both public and private sectors in these endeavors. Mauritius is top ranking regarding African nations and 14th worldwide,

by the ITU Global Cybersecurity Index (GCI) released in 2018 (14).
It has set up a National Disaster Cybersecurity and Cybercrime Committee that includes both public and private sectors and facilitates the monitoring, control, and transmission of decisions during cyber crises. Mauritius is one of the eight African countries to have ratified the Malabo, with which their Computer Misuse and Cybercrime Act is aligned, along with the Budapest convention on cybercrime. Mauritius has constructed a principal portal to register cyber incidents and a security intelligence center to identify and invigilate mischievous traffic instantaneously to ensure cyber security readiness nationwide (15).

V. EVIDENCE-BASED AND ACTIONABLE CYBERDEFENCE INTELLIGENCE AND RESILIENCE SYSTEM

Our findings showed that as health care personnel's and financial organizations are becoming more reliant on dedicated digital infrastructures and data-driven medical procedures , an abrupt cyberattack and subsequent shutdown can yield disastrous consequence in patient care, client and the enterprise/intuition all together. Cybersecurity, data security, and information assurance policies are of utmost importance for clinical laboratories to entirely be ready for potential cyber- attacks today and in the future as these is unavoidable in the digital age transformation (12)

Artificial intelligence (AI), deep machine learning (DML) technological innovations data mining and interpretation are which can be tailored into algorithms producing reliable predictive analytics, and for decisions making policies and practices can help in evidence-based decision support systems, efficient risk management, pattern recognition, cyber incident clustering, fore casting, malware identification and data safeguarding. For example, AI-based cybersecurity enabled application networks could sense vulnerabilities (bugs) and provide adequate threat response or quarantine there by strengthening, information system network security resilience.

Hence, further AI and DML-linked cybersecurity and cyber-wellness research and innovation (R&I) is no now the new normal in the digital era, to distillate the technological revolutions of AI-powered cybersecurity policies, due to its tremendous computing and processing power, tailoring complex algorithms for efficient security ecosystem, while addressing ethical and legal AI and digital issues and concerns.

VI. Combating critical infrastructures cyberattacks and cybercrimes

Recently, the development of the Nigeria's Cybersecurity Policy and Strategy, independent professional bodies like the Nigeria Computer Society and the Cybersecurity specialist/Experts Association of Nigeria provided feedback.

These clusters, whose enrollment intersect with public, private, and nonprofit actors as well as other decision makers from Nigeria's diaspora, enabling an upgraded technical skills, data sovereignty, and civic responsibility (11).

Practical and sustainable information logistics and dissemination management systems can be valuable in strengthening and securing transactions and deliveries. There is also need to explore vulnerabilities of electronic vehicle; electronic and grid security control units where attackers could potentially take control of these computer system or communication systems and manipulate the vehicle behavior causing accidents and other dangerous situations.

ISSN 2636-9680
eISSN 2682-9266

VII. BUILDING COLLECTIVE,EQUITABLE AND SUSTAINABLE CYBERDEFENCE OR CYBER-RESILIENCE SYSTEMS

Our findings showed an escalating number of cyber threats, eventually leading to difficulties to judicial prosecutors and legislative bodies in ensuring cyber security across the board and chiefly on critical infrastructures and cvber-equity.

Strengthening cyber-resilience requires investment in research, development, and the importation of international cyber security norms, which have proven its effectiveness for proper dissemination to national local regional sectors of the digital ecosystem justice.

African nations should proactively update and ratify a regional and national cybersecurity strategy to provide a comprehensive legal and framework, guidelines and mechanism on threat/crime surveillance, identification and incidence response for adequate protection and security of critical infrastructure.

These strategies should stipulate a nation-wide response plan during cyber-attacks, coupled with proper withdrawal strategies from cyber threats, ensuring both public and private sector should be capable of normal functioning even in the advent of sudden data loss during cyberattacks thereby, ensuring sustainability of quality cybersecurity service delivery in responses to cyber-attacks.

VIII. CONCLUSION

There is an emerging trend of cyber inequity between countries, corporates and organizations, evolving technological transition, current cyber-skills and workforce shortage leading toe increasing cyberattacks. Weak data and information privacy and rights protections concerns remain challenged due to ineffective national security, watchdog transparency and transnational enforcement laws and regulatory measures across Africa and worldwide. Leveraging on shared cybersecurity and cyberdefence collective partnership and governance framework, knowledge exchange, experiences and capabilities. This is crucial for proactive, resilient and sustained informed decisions and response actions against potential cyberattacks, crimes and vulnerabilities worldwide. Improving cybersecurity and other digital/electronic devices compliance guidelines, and or published data records, accounts and database long-term retention. It is necessary to develop and maintain policies and procedures to ensure high quality and better protection rights and security of individual, company and national security against unreasonable searches and seizure, and respect business rights.

IX. REFERENCES

[1] Kabanda G, Chingoriwo T. A Cybersecurity Culture Framework for grassroots levels in Zimbabwe. Orient.J. Comp. Sci. and Technol; Vol. 14(1-2-3) 17-34 (2021). Available from: https://bit.ly/3J1mQB2. W. P. Risk, G. S. Kino, and H. J. Shaw, "Fiber-optic frequency shifter using a surface acoustic wave incident at an oblique angle," *Opt. Lett.*, vol. 11, no. 2, pp. 115–117, Feb. 1986.

[2] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. Cybersecurity data science: an overview from machine learning perspective, 2020. Journal of Big Data. https://doi.org/10.1186/s40537-020-00318-5.

[3] World Economic Forum. Global risk report. 2020. https://www.weforum.org/reports/the-global-risks-report-2020. Accessed 1st August 2022.

[4] Shevchenko PV, Jang J, Malavasi M, Peters GW, Sofronov G, Trück S. The nature of losses from cyber-related events: risk categories and business sectors. J Cybersecurity. 1 janv 2023;9(1):tyac016.

[5] Allison A, Chatzilia A, Canham D. et al. Cyber risk executive summary. Technical Report. London: Institute of Risk Management, 2014b.

[6] Allison A, Chatzilia A, Canham D. et al. Cyber risk resources for practitioners. Technical Report. London: Institute of Risk Management, 2014a.

[7] Statista (2022) Africa: number of internet users in 2022, available at https://www.statista.com/statistics/505883/numberof- internet-users-in-african-countries/.

[8] Daniel Batty & Ethan Mudavanhu , (23 JUNE, 2022).The State of Cybersecurity in Africa: The Chinese Effect.

[9] Lesotho Times (2022), National Assembly approves cybercrime bill, available at National Assembly approves cyber-crime bill – Lesotho Times (lestimes.com).

[10] ITU (2021), Are African countries doing enough to ensure cybersecurity and internet safety, available at https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/.

[11] Abdul-Hakeem Ajijola and Nate D.F. Allen (March 8, 2022). African Lessons in Cyber Strategy. https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/.

[12] Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, et al. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Lab Med. 4 janv 2023;8(1):145-61.

[13] Saleous H, Ismail M, AlDaajeh SH, Madathil N, Alrabaee S, Choo KR, Al-Qirim N. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digit Commun Netw. 2022 Jun 23. doi: 10.1016/j.dcan.2022.06.005. Epub ahead of print. PMID: 35765301; PMCID: PMC9222023.

ISSN 2636-9680
eISSN 2682-9266