International Journal of Cyber-Security and Digital Forensics (IJCSDF) 6(3): 126-138
The Society of Digital Information and Wireless Communications (SDIWC), 2017 ISSN: 2305-0012

Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa

Ernest Tambo[1,2*] , Kazienga Adama[3]

[1]Africa Disease Intelligence and Surveillance, Communication and Response (Africa DISCoR) Institute, Yaoundé, Cameroon

2Higher Institute of Health Sciences, Université des Montagnes, Bangangté, Cameroun

3 Department of ehealth and Telemedicine Management, Rome Business School, Rome, Italy

*Corresponding author: tambo0711@gmail.com

Abstract

The rapidly growing broadband internet and mobile applications penetration and uptake provide immense opportunities and challenges across Africa. There is an increasing concern to national and regional security due to incidence and impact (cost)of cybercrime emergence and spread, cyberespionage and attack (e.g., hacking, hijacking or illegitimate and illegal use) of governments, private and public firms and other stakeholders' domains endangering healthy business, survival and performance opportunities in most African countries. Yet, only 11 (20.3%) out of 54 countries has implemented cybersecurity (CS) laws and regulations. Promoting cybersecurity and cyberspace preparedness and rapid response initiatives, preventive and protective countermeasures are vital and imperative. The rise of the digital economy is not just changing how organizations conduct business. Cybersecurity is a strategic decision by governments, industries, businesses and consumers driving this change need to step up their capabilities and be accountable for cyber-attacks, hacking, automated frauds and epidemic proportions of ransomware worldwide. Here, authors analyzes cybercrimes and mobile money frauds activities in most affected African countries and highlights practical and cost-effective awareness and capability approaches and strategies in building and establishing local and regional cooperation and collaboration for secured,effective and sustainable cyberspace information and data sharing and business transactions. Moreover, promoting personal data and information rights and privacy to e-commerce/e-transaction legislations and regulations best practice is crucial against cyber-attacks and its impact, in increasing productivity and sustainable economic prosperity in Africa.

Key words: Mobile money, cybersecurity, cybercrime, rights, privacy, cyber-legislation, surveillance, data, evidence, monitoring, Africa

Introduction

Cyber-security (CS) is a major concern to national and regional security in most African countries, governments and investors since the adoption of CS declaration by African Head of states at the "Africa Union (AU) convention on cybersecurity and personal data protections" in June 2014, Malabo, Equatorial Guinea. Thus far, only 11 (20.3%) out of 54 countries has implemented their CS laws and regulations [1]. The CS aims at protecting personal and public/private firms' data and database intellectual property rights (IPR), computer and data sharing network standards and benchmarks. It also seeks to harmonize cyber legislations on ecommerce, data protections and CS promotion from any incidence of cyber-crimes, cyberespionage and terrorism, hacking, hijacking or illegitimate and illegal use of private and public domains [1,2]. Contemporary, the rapidly growing broadband internet and mobile applications penetration and uptake across Africa has been challenged by the increasing emergence and spread impact of cybercrime/attacks on governments, private and stakeholders firms endangering healthy business, survival and performance opportunities [1,2]. At the same time, there is an increasing cybercrime incidence and impact (cost) in Africa due to lack of cybersecurity initiatives, lack of preparedness and countermeasures to deal with information security threats and cyber criminality strategies (forecasting, detection, response and control/containment) [3].Optimizing standards applications, data protection and privacy and lack of regulations and policies is crucial in boosting personal and organizations data and information security, awareness and risk communication on potential inside and outside vulnerabilities or attacks and impact. Our data showed that there is a growing internet penetration and users in Africa ranging from Kenya (69.07%), Mauritius (62.7%), South Africa (52%), Nigeria (47.9%), Algeria and Egypt shared 40% each. The most commonly incidents or cyber-crime cases ranged from web applications attacks and malwares, hackers and hijackers spread of ransonware, user names and passwords to pins, modify log in and social security number to spam emailsand social media abuse among others. South Africa and Morocco topped the incident count list followed by Uganda, Egypt and Mauritius with estimated costs of cybercrime impact of US dollars $573, 25, 35, 172 and 30 million respectively in 2016. Moreover it is documented that Kenya and Algeria have had huge economic loss on their GDP of $175 and $225 million with relatively incident of 27,172 and 10,790 incident cases in 2016 compared to top listed African countries. The impact of incident of cybercrime or cyber-attacks including malwares is colossal including huge financial lossestimated at approximately US $2 billion dollars in 2016 only in Africa [3,4]. In general the rate of global cybersecurity index (GCI) at country-level was relatively weak with low global ranking index on cybersecurity readiness based on legal measures, technical measures, organizational measures, capacity building and international cooperation assessment(Table 1)

Table 1: Pattern of cybercrimes and mobile money frauds activities in most affected African countries

Country	Population (million)	GDP per capita ($PPP)	Institution (Bank) account (%)	Internet users (%)	Mobile money account (2016)	Inter country mobile money	Incident count (cases)	Estimated cost of cybercrime ($million)	Common mobile money transactions in Africa	Common CS and mobile money transactions challenges and issues
South Africa	54.95	13,179	70	52	27-35% (5-7 million	Yes	220,727	573	Cash in / Cash out Airtime top up/ e-top-up Digital merchant payment and bill payment (utilities, transportation, school fees, hospital bills, utility and media bills, e-commerce or retail service payments, hospital bills) Payments of salary and pension, taxation and insurance payments). Other bulk payment P2P/G2P and third-parties and signing partnerships with other players such as: banks, insurance companies,	Lack of technical know-how inability to monitor and defend national networks rising incidence of cyberespionage and cyberterrorism Malware and malicious applications targeted banks and other firms CS unpreparedness and reliance on traditional fraud detection unpatched systems and insecure applications
Morocco	33.33	8,360	41	34.1		Yes	106,144	25		
Uganda	34.85	2,067	44	28.6	51%(7.7 million)	Yes	63,234	35		
Egypt	92.83	12,137	14	40.2		Yes	57,204	172		
Mauritus	1.26	20,525	82	62.7		Yes	52,974	30		
Kenya	45.53	3,360	75	69.07	>70% (26.7 million)	Yes	27,172	175		
Tunisia	10.98	11,657	27	28.6		Yes	25,665	NA		
Nigeria	173.0	5,930	44	47.9	43% (53.9 million)	Yes	20,158	50		
Zimbabwe	13.06	1,953	32	41.4		Yes	19,319	35		
Algeria	40.1	14,950	50	36.5		Yes	10,790	225		

									hotel booking and travel agencies, filling stations, super markets, Microfinance Institutions, etc	

GDP- Gross domestic product, PPP- Purchasing power parity (The global cybersecurity index (GCI) is a countrylevel global ranking index on cybersecurity readiness based on legal measures, technical measures, organizational measures, capacity building and international cooperation. The GCI does not seek to determine the efficacy or success of a particular measure, but simply the existence of national structures in place to implement and promote cybersecurity. The index has a low level of granularity based on country captured cybersecurity data and transactions commitment and preparedness, but not its detailed capabilities or possible vulnerabilities. The GCI ranged from 0 to 1.)

In addition, it is evident from the Figure 1 that the insider threat is the biggest security concern in African organizations and followed by attacks on computers and social engineering and utility theft in 2016. Insider threatrepresented 32% of overall cost due to cyberattacks while it was 26% and 15% for attacks on computer and social engineering respectively. We documented three are three main types of insider threats such as the malicious insiders, the exploited insiders and the careless insiders, while careless insiders are those who can accidentally cause damage or delete critical information by pressing wrong key. The smallest security threat by kind of attacks was the online fraud and scams at 8% of overall cost in 2016. Although the malicious insiders are the least frequent, they have the potential to deliberately steal information as well as cause damage due to their insider access. In contrast, the exploited insiders could provide sensitive data or password to external parties aimed at attacking the system (Figure 1).

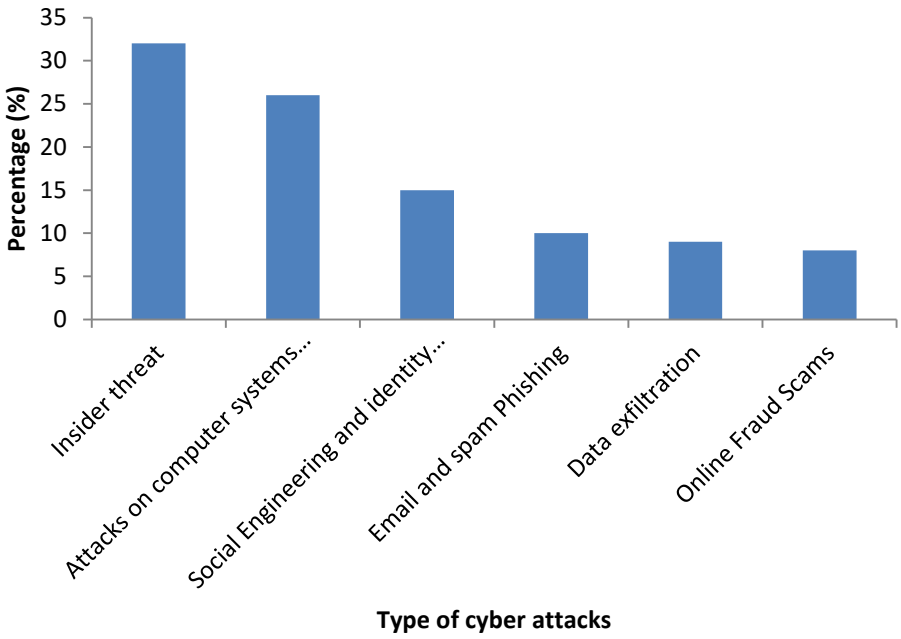

Figure 1: Distribution of the cyber-attacks cost per type of attacks in 2016 in Africa

Moreover, Figure 2 illustrated thepercent economic cost or loss due to cyber-attacks in Africa per industryin 2016. The Banking and Finance service, Government services and the E-commerce were the most affected and have been facing the greatest number of incidents cost list were 23%, 19%and 16% respectively.In banking sector, the banking malware, the ATM skimming and insider threat were the most common type of attacks, while it was website defacements, ransom demands and tax fraud for African government. In addition, the online fraud, the credit card fraud, we noted that the insider fraud and engineering malpractices were the type of cyber-attacks that caused significantdamages and losses in E-commerce and mobile base transaction sectors.

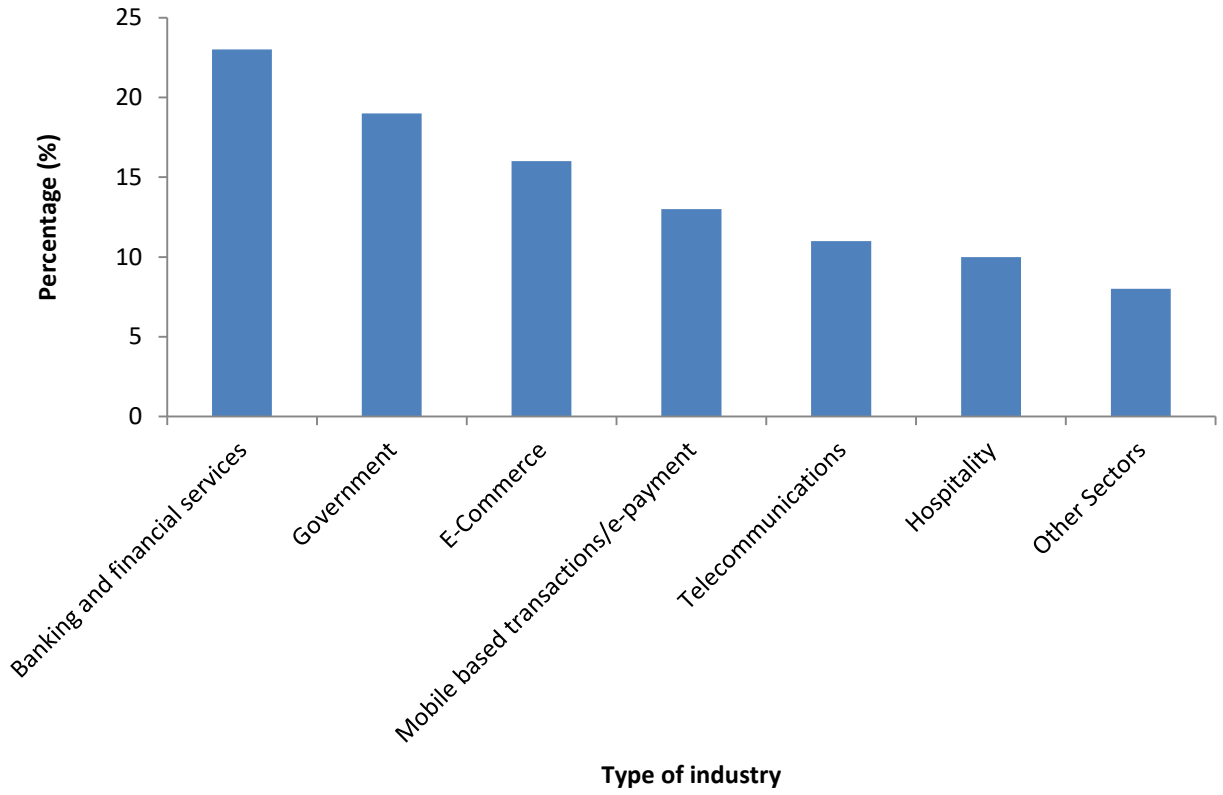

Figure 2: Distribution of the cyber-attacks cost per industry in Africa in 2016

There is an urgent need to reinforce regional and international comprehensive, context specific and integrated CS approaches and measures implementation, multi-stakeholders cooperation and collaboration including technical assistance in African countries. This is crucial in accelerating the implementation of the Malabo CS declaration policy, secured legislative framework and actions plans implementation [5]. Moreover, defining key CS terminologies, cyber legislation, policies and regulations) against cybercrimes and malwares impact in fostering regional CS and cyber-wellness (CW) in member-countries [5]. Nurturing national CS and CW engagement, leadership commitment, resource mobilization and investment approaches and strategies is needed in establishing local context CS enabling policies and laws. This is essential in formulating evidence-based cyberspace priorities and initiatives in ensuring digital technology and mobile applications security, CS and CW research and development innovations in accelerating local/global

financial security and economic prosperity. This paper aims at providing an overview of CS and CW opportunities and challenges in promoting public and communities CS and CW awareness campaigns and capacity development on information and technology risks including malware incidents, cyberattacks and ransomware, fraudulent transactions prevention and control capabilities en masse.

First, **there is an urgent need to promote CS and CW awareness campaigns on data and information security, citizen rights data informed consent and privacy, data sharing and monitoring of contextual performance and effectiveness management** against cyber-attacks and malware threats and impact. Moreover, evaluation of current CS preparedness capabilities is important in moving forward economic stability and sustainable development goals (SDGs) in Africa [1,2]. Fostering local and national Malabo CS frameworks, policies and regulations implementation at all levels is paramount to build and scale up resource mobilization, increases the risk of cyber-attacks awareness and social mobilization outreach, and citizenry education. Promoting CS and CW solid foundation of knowledge and lessons learned, skills development and knowledge empowerment approaches is of significance on internet technology and mobile applications services delivery on local and regional economy growth. Likewise, increasing community or citizenry awareness and education strategies on cybersecurity vulnerabilities and threats is paramount through online programs, media (Radio, TV) or trusted and reliable social media guidelines and instructions, comprehensive preparedness programs [1,2,5]. Moreover, cyberspace technical assistance and technology transfer training workshops and forums among government, private sector and stakeholders including community is important towards supporting risk management and decisions choice (s). Investing in cybersecurity capabilities development and implementation of is vital only after detecting an attack or reactive response, but mainly building organization cybersecurity information systems and monitoring tools.

Proactive and strategic local and regional CS policy, priority direction and access to resources is imperative for early threat hazard identification and threat analysis of all types of vulnerability of cyber/computer software and hardware attacks and life-threatening hazards. Moreover, enhancing CS resilience and expertise capacity

development to prevent, protect against, mitigate, respond to and recover from all cyber-attacks and hazards that affect the safety, wellbeing and economic security.

***Second,* local and international multi-stakeholders commitment and initiative(s)is critical in establishing country cybersecurity index (CCI)** readiness based on assessment of context specific technical and organizational requirements, local/national structures, regulations and legal measures, international technical cooperation, assistance and exchanges, capacity building and capabilities. CCI is of great value in cybersecurity surveillance data and transactions collection and analysis for timely cyber vulnerabilities assessment and early warning alert, promoting preparedness and evidence based response implementation [1,6]. Furthermore, implementing CS and CW monitoring and evaluation systems actions to determine the efficacy/performance or success to further improve local, regional and global security is vital.

***Third,* investing in CS and CW system is needed in developing and implementing effectively cybercrime approaches and investment** in Africa and globally. It's crucial to put in place cybercrime laws and regulation that transcends all boundaries aimed at ensuring confidence and trust in the use of internet including online transactions [1,3,6]. Furthermore, Genuine and sustainable governments, private industries and stakeholders efforts establishing a national leadership commitment and resource mobilization in integrated cybersecurity and cyber emergency response approaches and strategies capacity development degree programs, trainingand workshops seminars series to technical assistance for empowerment and resilience is also of crucial importance. Likewise, fostering national and regional CS collaboration and synergy in scaling up efforts in reducing and/or combating indiscriminate cybercrimes/-attacks at personal, private, public organizations and international levels [1,5] (Table 2).

Table 2: Summary of key cybersecurity core capabilities and activities

Cybersecurity Core Capabilities	Activities and Opportunities
	Policy, regulations and frameworks planning

Preparedness and Prevention	Public information screening, detection and early warning Operational coordination, access Control and identity verification Cybersecurity intelligence and Information Sharing Risk management for protection programs Supply chain integrity and security and physical protective measures
Mitigation	Mitigate existing and potential CS incident impact Public Community social mobilization ad awareness Long-term CS Community resilience and vulnerability reduction CS risk and disaster resilience assessment CS threats and hazards capacity building and trainings
Response	Critical response, health data and information safety Respond to CS incidents, cybercrimes and attacks or internet frauds CS infrastructure systems and workforce management Supply chain management logistics and public CS operations Laws enforcement and operational Communications Public healthcare and emergency services situational assessment
Recovery	Economic recovery health and social Services Housing and infrastructure systems Natural and cultural resources

Improving and sustaining current CS and mobile money services capabilities requires ongoing preparedness and response capacity development, trainings and exercises (drills scenario) activities important to ensure effective emergency response as well as promoting prevention to recovery or restoration programs for socio-economic and financial activities power and growth. There is need for Africa institutions and governments to promote and strengthening CS intelligence and information sharing and support necessary physical, technological, and cyber measures. It is needed for continuous CS public forensic tracing or sensor technologies analysis, digital, and/or biometric evidence within 24 hours of an attack to identify the perpetrator(s) and prevent or gathering priorities in response to a dynamic threat or future attacks follow-on acts and/or swiftly develop counter-options. This is important in providing timely,

accurate, and actionable information resulting from CS and CW planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback in order to develop innovative initiatives to mitigate the effects of future incidents and cyber-threats (Table 2).

***Fourth*, strengthening capacity development in CS and CW implementation framework in securing cyber space is crucial for states to harness information and communication technology (ICT), mobile health services**, mobile money and social media advantages and benefits in increasing economic, political and social productivity spheres [1,2,6,7]. There is an urgent need to fill the gap of CS experts or certified professionals shortage, lack of knowledge about the type and range of uncertainties, a high level of complexity, the nature of connections between entities, and little opportunity to predict future events by investing in universities and organizations related to research and development in security by creating of new degree programs in security in Africa (Table1). Ensuring stable and consistent secure cyber space needs development of new cyberspace knowledge and know-how capacity, building consistent data and effective metrics related to cyber-attacks, CS degree programs educationaland trainingprogramsinuniversities,and empowerment both students and professional careers development as well as supporting ICT and social media platform resources [1,2,5,7]. There is an urgent need to build sustainable capacity and capability in digital security intelligence and analytics that empowerment to rapidly detect, respond to and neutralize cybercrimes/attacks negative consequences and economic losses across Africa and worldwide.

***Fifth*, fostering research and development in CS, digital forensic and monitoring and evaluation is crucial towards achievement** of a secured and reliable cyberspacein Africa. Such operational CS research will provide local financial organizations, universities and organizations opportunities to develop a robust cyber and mobile money ecosystem policy, a vibrant digital and ICT security, privacy, accountability and transparency. Likewise, strengthening African institutions capabilities to protect, prevent and defend their infrastructure, coordinated, prompt, reliable and actionable information and services against internal or external cyber-attacks, e transactions and internet frauds crimes. Preventing cyber-attacks and frauds involves intelligence and deterrence operations; heightened inspections; improved surveillance and security operations; investigations; education and training; enhanced advanced digital technology detection capabilities; Financial and public health technologies surveillance, and testing processes; and law enforcement operations is core through implementation and reviewing constantly risk-informed guidelines consistent with national and international standards to maintain compliance, regulations and standards. But also, to ensure resilient and reliable public and financial institutions

security, reliability, integrity and availability of critical data and information, records and communications systems through collaborative and coordinated cybersecurity efforts including enforcement agencies to detect malicious activities. Response activities include: applying intelligence and other information to lessen the effects or consequences of an incident; increasing security and law enforcement operations; continuing investigations into the nature and source of the threat; continuing surveillance and testing processes; and allowing appropriate and sufficient community preparedness and response capabilities.

***Sixth*, addressing CS and mobile money multiple challenges and issues that African countries are facing is** crucial due to lack of local/regional cyber security surveillance and monitoring of incidence cyber-attacks (e.g. WannaCry), cyber-espionage and cyber-terrorism know-how and shortage of skilled cybersecurity professionals. Cyber-attack/crime is the fastest growing crime showed that without a effective and robust intelligence cyber defense development and implementation, it is estimated that cyber crime impact will cost over $6 trillion annually by 2021 with over 20 billion online consumers or users worldwide. Accelerating CS resource and capacity is essential in increasing CS security through infrastructure and human specialized training and resources strengthening, increasing internet/social media security and risk assessment, access control monitoring, confidentiality and authentication credential management. Others challenges and drawbacks include societal digitalization and globalization, mobility and heterogeneity of devices, expensive and specialized CS hardware-based tools, big data volume, velocity and variety of data, reporting and sharing of data policy and best practice, Moreover, the lack of legal and regulatory framework practices to prevent and fight cybercrime, private and public security systems consent directives and best practices, audit collection and privacy, communication and monitoring in taking effective and trustful counter-measures in neutralizing any threat [1,5,8,9]. Hence, building CS network of cooperative relationships, collaboration and community involvement is imperative across Africa. With the rapid growth of internet and mobile devices users within and across Africa, there is an urgent need to enhance authentication and access control in diverse portals and networks taking into account factors related electronic data fluidity, persistence stress and changing environment [1,10,11,12]. This requires new mobile money and internet of things safety and security innovations and measures across-industries strategic approach and intelligence sharing mechanisms in order to avoid financial and economic destabilization and fraudulent online business transactions impact on hard-won national economic transformations and gains. However, implementing cybersecurity best practices across an increasingly unstructured and decentralized network is one of the most difficult challenges facing companies and governments. Consumer-driven technology and artificial intelligence systems interconnected systems drives new devices and monitoring organizations are losing control of traditional security methods over online users and social media

networks. Cybersecurity R&D on emerging landscape and best practices need to reevaluate and establish contextual users security and trust capabilities from bottom-up improvements, device to level perspective instead of centrally-controlled, top-down actions [13,14]. Establishing and strengthening robust, reliable and CS resilience capabilities across all communities in Africa and worldwide is wealth and present multifaceted benefits to prevent, protect against, mitigate, respond to and recover from the public cyber-threats and hazards impact over time [15]. Lastly, Scaling up funding investment and collective efforts should be devoted to establish CS surveillance, resilience indicators and benchmarks in guiding evidence-based high value information and services assets, monitoring and evaluation of effectiveness against crippling of computer machines, outbreak of sophisticated cyber-attacks and digital ransom collateral damages worldwide.

Conclusions

There is an urgent need to increasing cybersecurity capabilities and cooperation by investing in building secured, reliable and sustained cyber space decision making platforms and frameworks. Unleashing CS leadership role and commitment is necessary to establish a CS and operating platform of all stakeholders including Microsoft, Google, Apple, Facebook, Banks, governments, and others private sectors on cyberattacks incidents affecting local and global market and share losses. Strategic CS and CW innovations on technologies and tools development and implementation needs, and organizational management are capital for societal benefits in Africa. This is crucialin reducing cyber-attacks and malwares threats and evolving challenges incidence and averting the colossal financial and socio-economic impact. Robust public and private big data and cybersecurity partnership and investment efforts are crucial in defining optimal and effective CS and ICT capabilities and requirements (e.g.: indicators, standards ad benchmarks) integration, knowledge and skills development against CS intruders and other mobile money threats. Building public and community CS communication and engagement resilience, readiness and capability is crucial in promoting public and community CS and CW policy and capabilities, awareness campaigns and engagement and empowerment in reducing cybercrime. Evidence-based event-specific CS laws and regulations implementation is also needed in ensuring safe and effective electronic or digital commerce/transaction cyber emergency implementation, personal data and information rights and privacy laws. As well as building trusted and reliable cyberspace and cyber-security environment including cyberforensic data sharing, research and development agenda in guiding effective preparedness and best practices actions including early detection ,timely protection and response or countermeasures modeling, monitoring and evaluation to cybercrimes/attacks consequences on Africa productivity and economic prosperity.

Author contributions

ET conceived the idea and performed the preliminary search and wrote the outline. AK prepared the table. ET, AK and HFS provided additional contextual information in Africa. ET thoroughly revised the manuscript. Authors read and approved the final version.

Conflict of interest

Both authors have no competing interests.

Funding

No funding was received

References

1. Waldrop MM. How to hack the hackers: The human side of cybercrime. Nature 2016, 12;533(7602):164-7.

2. African Union Directorate of Information and Communication, "Press Release Nº18/23rd AU SUMMIT, The 23rd Ordinary Session of the African Union ends in Malabo," press release, 30 June 2014,http://summits.au.int/en/sites/default/files/PR%2018%20-%2023rd%20AU%20A...(3).pdf

3. African Union, http://au.int/en/cyber legislation(accessed 12th March 2016) 3. Draft African Union Convention on the Establishment of a credible legal framework for cyber security in Africa. African Union, http://au.int/en/cyberlegislation (15th March 2017)

4. Ephram Percy Kenyanito. Africa moves towards a common cyber security legal framework. https://www.accessnow.org/africa-moves-towards-a-common-cyber-security-legal-framework/ (accessed 27th March 2017)

5. Canetti D, Gross M, Waismel-Manor I, Levanon A, Cohen H. How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks. *Cyber psycho Behav Soc Netw*; 20(2):72-77 (2017).

6. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol Health* Care; 25(1):1-10 (2017).

7. Mackey TK, Nayyar G. Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. Br Med Bull; 118(1):110-26 (2016).

8. Ropp R, QuammenB. Build your defense! Develop a strategic plan of action to combat cybercrime. Health Manag Technol;36(10):8-9 (2015).

9. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: A systematic review. Technol Health Care. 24(1):1-9 (2016).

10. Canetti Daphna, Gross Michael, Waismel-Manor Israel, Levanon Asaf, and Cohen Hagit. How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks. *Cyberpsychology, Behavior, and Social Networking*; 20(2): 72-77 (2017).

11. Aransiola JO, Asindemade SO. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychol Behav Soc Net, 14(12):759-63 (2011).

12. Yaghoobi A, Mohammadzade S, Chegini AA, Yarmohammadi Vasel M, Zoghi PaidarMR. The Relationship Between Attachment Styles, Self-Monitoring and Cybercrimein Social Network Users. Int J High Risk Behav Addict. 5(3):e27785 (2016).

13. Check Hayden E. Cybercrime fight targets user error. Nature; 518(7539):282-3 (2015).

14. Ernest Tambo, Ghislaine Madjou , Christopher Khayeka-Wandabwa , Emmanuel N. Tekwu , Oluwasogo A. Olalubi, Nicolas Midzi , Louis Bengyella , Ahmed A. Adedeji , Jeanne Y. Ngogang. Can free open access resources strengthen knowledge-based emerging public health priorities, policies and programs in Africa? *F1000Research*, 5:853 (2016).

15. Tambo Ernest, GhislaineMadjou, Yves Mbous, Oluwasogo A Olalubi, Clarence Yah, Ahmed A Adedeji and Jeanne YonkeuNgogang. Digital health implications in health systems in Africa. *Eur J of Pharmaceutical and Medical Research* 2016,3(1), 91-93