International Journal of Science Academic Research
Vol. 04, Issue 07, pp.5926-5931, July, 2023
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

SYSTEMIC LITERATURE REVIEW ON CYBER INSECURITY IMPACT ON THE AFRICAN ECONOMY

***Emmanuel Eturpa Salami, Tijani Lucky Abdulsalami, Clement Onyemaechi Nwakbuokei**

Department of Computer Science and Information Technology, College of Natural and Applied Sciences,
Igbinedion University Okada, Edo State, Nigeria

Received 25th May 2023; **Accepted** 20th June 2023; **Published online** 30th July 2023

Abstract

The rapid growth in technological advancement and adoption of digital electronic transaction gateways have had profound impact on global economy but this is not without the attendant security risk. The entire human ecosystem is managed through the adoption of ICT and the benefits are evident in the healthcare system, economy, education, political and businesses sectors globally. Cyberspace has become the converging point for information sharing and management as well as a platform for governments, cooperate organizations and individuals to harmonize their common goals. It is also a platform for information warfare involving state actors, business managers, and domain experts. The objective of the research is to investigate the threats and natures of cybercrimes and their impact on the African economy with a particular focus on Nigeria, and Ghana. A systemic literature review methodology was used to provide an in-depth understanding of the economic impact of cyber insecurity on the African continent. The estimated cost of cyber-crime in Africa is put at $895m which has continued to soar with Nigeria losing about $550 million to cybercrime, Kenya ($175 million), Tanzania ($85 million), Ghana ($50 million), and Uganda ($35 million) each on a yearly basis. The study recommends the adoption of a more proactive and defensive cybersecurity resilience approach through the strengthening of existing cybersecurity policy frameworks and implementation strategy, rather than the reactive approach which has been the case in most developing countries. The need to be more deliberate in investing in training well-skilled Domain experts as well as providing infrastructures that support cybersecurity defense cannot be over-emphasized.

Keywords: Cyberspace, Insecurity, Threats, Cybersecurity.

INTRODUCTION

The transit from the industrial age to the digital age comes with its unique problems and the top among these problems is the safety and security of the digital space and channels of conveying information. Both physical security and cybersecurity have varying challenges which impact the digitalization of international and national economies globally. Critical infrastructures and virtually all economies in the world today are dependent on network connectivity as most business and government operations are now performed via cyberspace. Cybercrimes have increasingly become very attractive thereby heightening the cases of cyber insecurity globally. System tech cyber report of 2012 reveals that cyber-attacks alone cost US$114 billion each year and it is projected to reach US$385 billion, the survey was conducted across 24 countries [8]. The effect of cybersecurity will continue to have a severe impact on businesses and governments globally. Today ransom ware attacks are becoming more prevalent and some of them are evasive to detection because the perpetrators of these crimes seem to be way ahead with the sophistication of attack tools that are readily available to them. Cybercriminals capitalize on system vulnerabilities, ignorance, and gullibility on the part of users to perpetrate their heinous crimes. Between 2006 and 2007, financial losses occasioned by cyber crimes in the United States alone increased dramatically from $52.5 million in 2006 to $67 million [15]. Internet connectivity makes it much easier for criminals to act beyond national boundaries when conducting their illegal affairs. With over 300 countries connected to the internet and still counting, cybercrime has become a global issue that requires a multi-stakeholder effort including governments, the private sector, civic and legal institutions, and other social organizations. Even though cyber insecurity is a global issue, developing nations such as Africa and some Asian countries are more vulnerable to the insecurity emanating from cyberspace because of their level preparedness in transiting into a fully digitalized economy has not been well coordinated. The South African economy alone lost about $242 million USD in 2013 as a result of cybercrime, also on the African economy in 2016 lost at least $835 billion in cybercrime alone [14]. The question as to how prepared the African nations are in dealing with cyber insecurity is yet to be sufficiently answered, though policies and cybersecurity frameworks have been designed and even given legal backing in some African countries the problem, however, has always been the willingness to implement, the lack of resources and tools in terms of trained professionals in the domain of cybersecurity and technological tools to address the issue. For the African economy to really maintain a steady growth as one of the fasted growing economies it must properly address the rising issue of cyber insecurity. The aim of this paper is to provide and analyze what the trends are and interrogate the issues from the global perspective while narrowing it down to the African economy with a particular focus on Nigeria. The objective of the study is to The alarming cases of cyber crime targeting the African economy in recent times making it very imperative to demystify and suggest ways through which the issues can be addressed so that it does not overwhelm both policymakers and businesses to extend that it sabotages the growing African economy. Looking at the trends within African cyberspace today how secure are the businesses and government-owned infrastructures that must conduct their operations highly depending on cyberspace? A hybrid research methodology that includes a review of literature, reports, journals, and pre-recorded surveys were carried out for an in-

Corresponding Author:** ***Emmanuel Eturpa Salami,
Department of Computer Science and Information Technology, College of Natural and Applied Sciences, Igbinedion University Okada, Edo State, Nigeria

depth analysis of the current trends and challenges of cybersecurity as it affects governments, businesses, and individuals globally.

Literature review

The cyber threats landscape is growing by the day with various types of threats immerging especially with the fast pace of technological advancement. Insecurity has taken a different dimension from the conventional. The challenge with the African continent is the lack of talent and resources to deal with cybersecurity threats unlike what is obtainable in most European and Asian continents where there is an aggressive approach toward developing talents that will help in maintaining the safety of infrastructure and people. The author [2] observed that the rise of supply chain threats and escalating ransomware attacks are the most pressing cyber challenges the international community needs to address. Business leaders must consider cybersecurity as a risk management issue and balance the trade-offs between security, usability, and cost at the Board level.

In 2021 an average of 270 attacks was recorded per organization globally which shows a 31% increase from 2020 and the top three cyberattacks were infrastructural breakdowns as a result of a cyber-attack, identity theft, and ransom ware. However, most cooperate organizations are fast embracing the transition to cyber resilience as an alternative to the traditional cyberattack approach adopted in the past as reported by the World Economic Forum in 2022 [4]. The major areas of focus in 2022 for businesses and security-focused executives in the cooperate world are in the listed areas in Table 2.1.The impact level as shown will determine how much resource would be committed according to the global cybersecurity outlook of 2022.

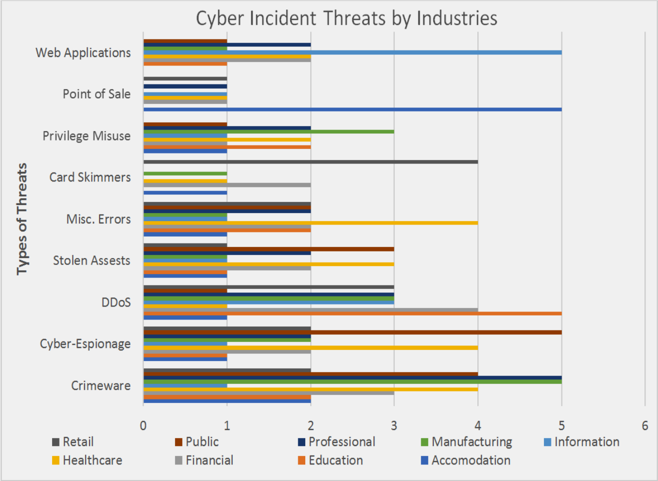


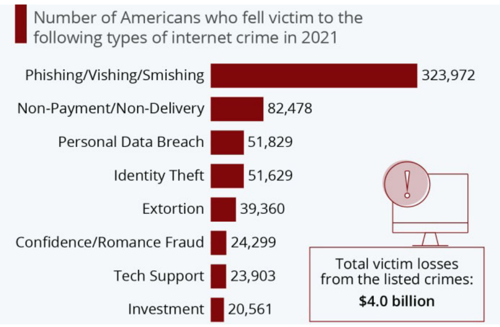
Figure 1. Cyber Threats Statistics Impact by Industry

The chart in Figure 1 shows the cyber statistics and trends and how severe each trend is to the different industries. On a scale of 1 to 5 where (1=Very low, 2=low, 3=medium, 4=medium high, and 5=high). Crime ware as a cyber-attack is seen to be high in both the professional and manufacturing industries, while espionage attack is recorded as the highest type of attack in public industries such as government-owned businesses since such attacks are usually targeted at disrupting the economy, reputation, and infrastructure of perceived enemy nations. The growing cases of Distributed Denial of service (DDoS) are more prevalent in the educational sector as seen from the chart.

Global Perspective on Cyber Insecurity Threat Impact

From a global standpoint, most European countries have risen up to address the rise in cyber insecurity. Countries like Germany, France, and the United Kingdom between 2006 to 2008 upgraded their existing cyber security laws and frameworks though [8] the decision taken by these countries did not capture the core strategy that could deter cyber criminals rather it focused more on mitigating the effects alone. According to the report [13]. Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015. At a growth rate of 15 percent year over year Cybersecurity Ventures also reports that cybercrime represents the greatest transfer of economic wealth in history. Brazil's blackout in March 1999 left nearly 70% in the dark for more than 5 h affecting over 97 Million citizens. In 2003, left parts of the US and Canada in chaos, leaving them high and dry without power. In a matter of minutes, many places in Pennsylvania, Massachusetts, New York, Connecticut, New Jersey, and Ottawa went dark. The darkness caused the public transport system to go out. Many utility corporations were shut down due to this power shutdown and forcing emergency services like hospitals to run on limited power [26]. In 2003, slammer worm aka Sapphire disrupted Ohio Nuclear Plant [10]

A recent report made available by the Federal Bureau of Investigation (FBI) on internet crime reveals that more than three hundred thousand Americans have fallen victim to at least one of the listed cybercrimes in figure 2.1 with Phishing, Vanishing, or Smishing attacks in 2021 alone [7]. Cybersecurity Ventures (2021) reported that global cybercrime costs are expected to increase by nearly 15 percent on a yearly basis over the next four years to reach $10.5 trillion annually by 2025, from $3tn in 2015. In terms of geopolitical cyber warfare, some state-sponsored actors are likely to use cyberspace as a medium to damage the reputation of other nation-states and even disrupt infrastructure operations as a way of destabilizing the economy of such states, and this simply because of the affordability, reliability, portability, and difficulty in detection of some of these operational technologies used for cyber-attacks.



Source: FBI's Internet Crime Complaint Center

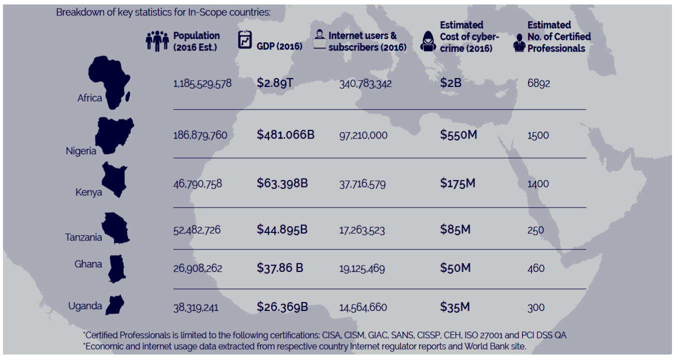
Figure 2. Types of Internet Crime and number of victims in America

Table 1.Cybersecurity Focus for 2022

Threats/ Attacks	Percentage Impact
Personal assets	10%
Ransomware attacks	20%
Identity theft	24%
Infrastructure	42%
Others	4%

African Perspective on Cyber Insecurity Threat Impact

In November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, [11] listed 11 countries in the continent that already had specific laws and provisions in place to deal with cybercrime and electronic evidence: Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda, Zambia, and 12 other countries had taken at least some legislative measures, albeit limited. Draft cybercrime laws had been prepared in many other countries and bills had already been presented to national Parliaments in some of the countries however, the big challenge has always been implementation. The internet economy is expected to contribute $180 billion to the African continent by 2025 and it is projected to rise to $712 billion in 2050 according to the report from International Financial Cooperation however if cyberspace is not adequately secured, the economic impact will be very devastating. African GDP was reduced in 2021 by 10% as a result of cybercrime and the list of countries that experienced a severe hit were South Africa, Nigeria, and Ethiopia as shown in figure 2.3. In 2020 it was South Africa suffered a huge loss of $147 million as a result of cybercrime which made it to be ranked third highest with the record of cybercrime victims globally while Nigeria reported cases of malware-infected applications particularly those running on Android Operating Systems was at it highest in the same period [2]. There is a wide gap in terms of cybersecurity professionals' talents in the continent, only 7,000 people are certified as security professionals in 2018 1.24 billion people in Africa. The author [2] identify cybercrime as one impediment that will have a severe impact on the African economy as the continent is transitioning to E-commerce under the Africa Continental Free Trade Area (AFCFTA) and this impact is a result of domestic regulations that are were enforced without any consideration of global nature of cybersecurity by some Africa nations. Also, the slow implementation of the Malabo Convention on cybersecurity and personal data protection which is aimed at mitigating the threats of cybersecurity. Most African countries have come under severe criticism from international organizations because the investment and attention that is given to cybersecurity issues in terms of provision and implementation policies and laws have been grossly inadequate, particularly the private sectors seem not to be doing more implementing relevant cybersecurity laws that being passed by the legislators.



Breakdown of key statistics for In-Scope countries:

	Population (2016 Est.)	GDP (2016)	Internet users & subscribers (2016)	Estimated Cost of cyber-crime (2016)	Estimated No. of Certified Professionals
Africa	1,185,529,578	$2.89T	340,783,342	$2B	6892
Nigeria	186,879,760	$481.066B	97,210,000	$550M	1500
Kenya	46,790,758	$63.398B	37,716,579	$175M	1400
Tanzania	52,482,726	$44.895B	17,263,523	$85M	250
Ghana	26,908,262	$37.86 B	19,125,469	$50M	460
Uganda	38,319,241	$26.369B	14,564,660	$35M	300

'Certified Professionals is limited to the following certifications: CISA, CISM, GIAC, SANS, CISSP, CEH, ISO 27001 and PCI DSS QA
'Economic and internet usage data extracted from respective country Internet regulator reports and World Bank site.

Source: African cybersecurity report 2016

Figure 3. African cybersecurity report

Cyber-crime and Cyber Insecurity in Africa

Cyber-attacks are serious threats to both the economy and national security of any nation. Africa has also had a fair share of various Cyber-crime cases which has further heightened the problems that the continent is experiencing in term of cybersecurity. An instance is the fraudulent cyber activities which is believed to originate mostly from the West African coast, and are popularly called "advance fee fraud" is traceable to Nigeria. It is a type of Internet fraud used to defraud victims willing to succumb to the temptation offered to make some "quick money" [20, 9]. Skirmishes of these incidences are now been reported in other West African nations such as Senegal, Cote d'Ivoire, Cameroon, Sierra Leone, the Gambia, Benin Republic, and Ghana [25]. The frauds take the form of victims being approached by letter, faxes, or, recently, electronic mail, without prior contact. Victims' addresses are obtained from telephone and email directories, business journals, magazines, newspapers, or through web e-mail address harvesters [22]. Cybercrimes will increasingly be initiated from jurisdictions that have few laws directed against cybercrime and little capacity to enforce laws against cybercrime. This is the scenario in most of the Sub-Saharan African nations where some of these crimes are purported to emanate. Pati [26] noted that "the (de)creativity of the human mind cannot be checked by any law.

The problem of legal jurisdiction has also made tackling economic crimes perpetrated through cyberspace hard to deal with. Different countries within the African continent have different perspectives on existing statutes enacted over the past decades which shows varying and diverging jurisdiction clauses. However, some of these laws have not clearly defined how to address the extent to which a particular event in cyberspace is controlled by the laws of the country outside where the crime was, by the laws of the country where the Internet Service Provider is located, by the laws of the country where the user is located, or perhaps by all of these laws [3] while in some countries, a number of cybercrimes are yet to be captured by national laws.

Cyber attacks Vectors

Owing to the fact that almost all aspects of government and corporate organizations' business operations are fully becoming digitalized, the various platforms and service channels will experience an increase in attacks which will definitely have a major impact on the economy of nation-states. This will be even more serious in developing continents as their security structure are very weak and there are no structured ways of tracking most of the cybersecurity incidences that occur whether to government businesses or corporate organizations.

Cryptocurrency

Cryptocurrency exchanges experienced a 10-fold increase in attacks in the first half of the year compared with the prior year period and the majority of the cryptocurrency attacks were orchestrated through social media. Many more businesses that deal with cryptocurrency will remain a focal point of attack and this is because this has become a new medium of transaction of business both by government and corporate organizations and the majority of the activities and communication are taking place through social platforms [19]. In 2021, about $353 million in digital coins was stolen from Poly Network swapping platform just within 24 hours due to hackers' activity which shows the vulnerability of that platform [31].

Application Programming Interface (API)

Adoption and integration of the Internet of Things and 5G traffic will make API services and apps a lucrative soft target that attackers will explore because of their information exposure potential. These vectors have a high potential of introducing additional risk to businesses as attacks through them are not easily detected due to the low-level security controls most of them have.

Cloud Migration and Ransom ware

Businesses are migrating from traditional storage and usage of infrastructure to outsourcing some critical business functions to cloud service providers and can be traced to the pandemic era that necessitated a faster transition from what was the norm for business operations. However, being able to detect and prevent malicious activities in the cloud is a lot different from the traditional ways of doing them. The limited knowledge on cloud security and application by some organizational teams or government agencies can pose a high risk when migrating to the cloud and if not properly addressed, it has the potential of costing huge financial losses.

Cyber insecurity threat impact on Nigeria and Ghana

Chioma *et al.* [5] identify the lack of feasibility and workability analysis of some policies, sabotage by the regulatory agencies and elite class for personal gains, and poor funding of the security agencies as the root cause of an increase in cyber security in Nigeria. The cybersecurity Gap in Africa is a clarion call to African governments to step up the drive towards initiatives that will rapidly boost the connectivity and access problems across the continent. With the rapid urbanization in Nigeria with an annual population growth rate of 4.3% with a large population beginning Youths between the age of 16years to 45 years it has become more challenging combat cybercrime due the fact that the shortage of well-trained and experienced cybersecurity professionals. There are over 200 fintech organization today in Nigeria that provides online financial services and the security of these channel of financial services do not compile with global best practice thereby creating new frontiers for cyber attack on innocent subscribers whose financial information are housed on their solutions.

The high rate of youth unemployment and the absence of enforceable prohibitive laws and the poor awareness on cybercrime detection and prevention methods is another identified factor that has further increased cyber insecurity incidents within the Nigerian economy [14]. The study by Hassan *et al.* [14] also showed an increase in cases of cybercrime offenses among the youth as this has become a lucrative venture for these categories of the Nigerian population. Akwara *et al.* [3] observe that there is a positive correlation between unemployment, poverty, and cybercrime among Nigerian youths. The trends in cybercrime in Nigeria though known, the defensive approach has been very weak as most time only a few institutions such as the Economic and Financial Crime Commission (EFCC) as well as the Independent Corrupt Practices and other related offenses Commission (ICPC) are seen to be in the frontline of tackling cybercrime. The legal system on the other hand have not made this war against cyber insecurity much friutful because some of these cybercrime were not envisaged therefore adequate laws were not put in place to handle them. The economic impact of cybercrime particularly in the financial sector has affected the growth of the economy of Nigeria. This has led to slow growth in production, increase in overhead cost, monetary and privacy losses, reduction in Nigerian’s competitiveness in the global market as well as defamation of the country’s image globally. Geo-political tensions and military incursion have also been observed to trigger a cyber attack on critical national infrastructure. Stuxnet, for instance, was dissected and diagnosed as a pioneering and politically motivated cyber attack. Unfortunately, it successfully infiltrated a high-security, government-run critical infrastructure and destroyed its physical property with computer code. According to Warner [35], the Ghanaian cybercriminal infrastructure has been dominated by three major forms of cybercrimes: identity fraud, fake gold dealers, and estate fraud. Identity fraud in Ghana is also known as “romance fraud” whereby a person “hooks” a prospective lover/partner from the United States or Europe and convinces them to send funds to support their relationship [35]. This type of fraud has received the most attention in the United States and Europe contributing to “Ghana being blacklisted for money-laundering by the international watchdog the Global Financial Action Task Force in 2012” [11]. Cyber attacks on Critical Infrastructures (CI) in the petroleum sector over the past few years have raised with vulnerabilities in key infrastructure. Oil and natural gas utilities are part of the nation‘s CI. Kevin Hillmer-Pegram[14] itemized five (5) main phases of the activities associated with oil and gas production which are now areas of the target. They are as follows:

a) Leasing
b) Exploration
c) Development
d) Production and Transportation
e) Decommissioning and abandonment.

And each phase involves a complex network of actors from the governmental, private, and civic spheres of the society. Traditional Operational technology (OT) such as Industrial control systems (ICS), Process Control Systems (PCS), and others are typically used to monitor, automate, and control critical physical processes, such as physical access control. These control systems typically collect information about facility operations and specific component status and to checkmate, manage, command, direct, or regulate the behavior of devices or components. Attacks on any OT could disrupt supply, and trigger a physical event. In August 2017, for instance, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyber assault to sabotage the firm‘s operations and trigger an explosion. Many operators in the energy sector lay emphasis on increased expenditure on the security of their corporate IT systems; this has not been matched for OT systems, thereby leading to their increased attractiveness to cyber assailants [7]. Known cybersecurity risks affecting ICS consist of increased use of digital controls, removable data storage devices, system updates and patches, and insider threats. Nigeria being an oil-producing nation is not left out when it comes to such attacks coming from OT disruption. The problem of insecurity caused by the dreaded Islamic sect group known as Boko Haram in Nigeria has severely affected the economy of Nigeria even more worrisome is the cyber attack on the Nigerian government secret service database that was carried out by Boko Haram, this has further increased the fears by the western intelligence agencies on safety and reliability of information gotten from the Nigerian State Security Service (SSS) [1]. While in Ghana, an attack on a government website by a rouge group of Turkish hackers that led to the denial of access is a case of an external force compromising the security of another nation through cyberspace [1]. Adam, M. [1] observed that the Ghanaian government has not yet developed an official cyber security strategy and framework which will address these increasing cases of cyber-attacks that are gradually costing the nation huge losses both nationally and internationally. Adam Motiwala proposed the establishment of a central agency that will be solely devoted to research, articulation, and coordination of cyber security policies by the Ghanaian government as a way forward towards addressing the cyber insecurity within the Ghanaian system [1].

Conclusion

Cybercrime is a transnational and transborder crime that requires a collaborative approach in order to be able to mitigate it impact on the economy of any nation. Cyber insecurity is a significant issue for the African economy, with the potential to cause significant economic and reputational damage. As the use of new technologies and devices grows, and the threat of cybercrime increases, African countries must invest in cybersecurity infrastructure, training, and education to combat this threat effectively. Collaboration between governments, businesses, and individuals is critical to creating a safe and secure digital environment in Africa considering the impact of the cyber threats. It is essential that proper precautionary measures and defense mechanisms be employed in protecting critical infrastructures. The current posture of cyber insecurity impact as seen today goes beyond the traditionally known causes because of the rapid growth in the development and adoption of Information technology therefore, the African continent must keep up with the dynamics of these technological growths. In addition to this is the need for more Collaboration at the regional and subregional levels on capacity building and development. Governments must strengthen its partnerships with private organizations and other relevant bodies in drafting implementable cybersecurity policies that are contemporary to address the dynamics that technology brings into the national economy. Maintaining steady growth in the African economy will also demand that African Union develop a policy guideline to address transborder cybercrimes to reduce it occurrence.

REFERENCES

1. Adam, M. (2020). Cyber Security in Ghana: Evaluating Readiness for the Future. Retrieved 04 03, 2023, from https://www.wathi.org: https://www.wathi.org/wathinote-election-ghana-situation-securitaire/cyber-security-in-ghana-evaluating-readiness-for-the-future-kaiptc/
2. Adeboye, A., Boakye, B., and Garson, M. (2022). Cybersecurity in Africa: What Should African Leaders Do to Strengthen the Digital Economy? Institute for Global Change. Retrieved January 2, 2023, from https://institute.global/policy/how-rethink-cybersecurity-africa-strengthen-digital-economy
3. Akwara, A. F., Akwara, N. F., Enwuchola, J., Adekunle, M., & Udaw, J. E. (2013).Unemployment and Poverty : Implications for National Security and Good Governance inNigeria. *International Journal of Public Administration and Management Research*, 2(1), 1–11.
4. Brenner, S. (2007) Law in an Era of Smart Technology, Oxford University Press, Oxford.
5. Chioma, C.-O., Samuel, U., Daniel, M., and Osuo-Genseleke, M. (2017). The proliferation of Cyber Insecurity in Nigeria: a root cause analysis. *International Journal of Science and Technology, 6*(2). doi:10.4314/stech.v6i2.4
6. Center for Infrastructure Protection. (2003), Blackout: A Case of Study of the 2003 North American Blackout with Exercice. Available from: http://www.cip.gmu.edu/wpcontent/uploads/2013/10/ blackout-learner-version.pdf
7. Ciepiela, P. (2017). Digitization and cyber disruption in oil and gas, OT/IoT Security And Critical Infrastructure Leader, EYGM Limited, BMC Agency, GA. Cukier, W. L., Nesselroth, E. J., and Cody, S. (2007) Genre, Narrative and the "Nigerian Letter" in Electronic Mail. In Computer Society, Washington, DC, 70.
8. Economic Community of Africa, E. C. F. (2021). Cybercrime A barrier to Africa's thriving digital economy. Retrieved February 22, 2023, from https://www.uneca.org
9. Darko, S. (2015). “Inside the World of Ghana’s Internet Fraudsters,” BBC. www.bbc.com/news/world- africa-32583161
10. Felix, R. (2022). The Most Common Types of Cyber Crime. Statista. Retrieved 03 13, 2023, from https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/
11. Guitton, C. (2013). Cyber Insecurity as a national threat: overreaction from Germany, France and the UK. *Politics and International Relations Journals, 22*(1), 21-35. doi:https://doi.org/10.1080/09662839.2012.749864
12. Hassan, A. B. Lass F. D. and Makinde J. (2012) Cybercrime in Nigeria:Causes, Effects and the Way Out, *ARPN Journal of Science and Technology,* vol. VOL. 2(7), 626 – 631
13. (PDF) Cybercrimes in Nigeria: Analysis, Detection and Prevention. Available from: https://www.researchgate.net/publication/320411102_Cybercrimes_in_Nigeria_Analysis_Detection_and_Prevention [accessed Jun 29 2023].
14. Julian, J. J., and Surya N. (2014). *A Survey of Emerging Threats in Cybersecurity.* doi:https://doi.org/10.1016/j.jcss.2014.02.005
15. Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77-81. doi:https://doi.org/10.1080/1097198X.2019.1603527
16. Kevin, P. (2003). Slammer Worm Crashed Ohio Nuke Plant Network, (Security Focus). Available from: http://www.securityfocus.com/ news/6767. [Last retrieved on 2017 Dec 06].
17. Kevin, H. P., (2014). A synthesis of existing, planned, and proposed infrastructure and operations supporting oil and gas activities and commercial transportation in Arctic Alaska University of Alaska Fairbanks.
18. Lendvay. R. L., and Kiernan K. (2016). Shadows of Stuxnet: recommendations for U.S. policy on critical infrastructure cyber defense derived from the Stuxnet attack. PG Thesis, Naval Postgraduate School Monterey, California.
19. Longe and S. Chiemeke. (2006) The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam.
20. June Covenant University, Ota, Nigeria, 1 - 7.
21. Mclean, M. (2022). *2022 Must-Know Cyber Attack Statistics and Trends.* Retrieved from https://www.embroker.com: https://www.embroker.com/blog/cyber-

attack-statistics/

22. Oumarou, M (2007) Brainstorming advanced fee fraud: 'Faymania' – the Camerounian experience, in N. Ribadu, I.
23. Lamorde and D. Tukura (Eds), Current trends in advance fee fraud in West Africa, EFCC, Nigeria 33–34.
24. Pati, P. (2003) Cybercrime, New Delhi [Online]. Available: http://www.naavi.org/pati/pati_cybercrimes_dec03.htm [Accessed 23 February 2010]
25. Paula Musuva-Kigen; Martin Ekpeke; Emmanuel Inkoom; Beatrice Inkoom. (2016). *Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness.* Kenya: Serianu Limited, Turnkey House.
26. Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences,
27. Proceedings of the 40th Annual Hawaii international Conference on System Sciences, January 03 – 06, HICSS.IEEE
28. Robert, R. (2008). *Computer Crime & Security Survey.*
29. Reuters. (2021, 08 12). How Hackers pulled off the Biggest cryptocurrency heist from Poly Network. Retrieved 03 13, 2023, from Thenationalnews.com: https://www.thenationalnews.com/business/cryptocurrencies/2021/09/21/how-hackers-pulled-off-the-biggest-cryptocurrency-heist-from-poly-network/
30. Sharma, A. (2021, 12 29). *Top 10 cybercrime trends to watch for in 2022.* Retrieved 03 13, 2023.
31. Smith R. G., Grabosky P. N. and Urbas G. F. (2004) Cyber criminals on trial, Cambridge University Press, Cambridge..
32. World Economic Forum. (2022). *Global Cybersecurity Outlook 2022.* World Economic Forum.
33. Warner, J. (2011). "Understanding Cyber-Crime in Ghana: A View from Below," International Journal of Cyber Criminology, 5(1): 736—749.

****