World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Impact of cyberspace on the cybersecurity of critical national assets infrastructures in Nigeria: A review of education and financial sectors

BILLE David Urbanus *

Department of Security and Strategic Studies, Nasarawa State University, Keffi, Nigeria.

World Journal of Advanced Research and Reviews, 2022, 16(01), 595–604

Publication history: Received on 14 September 2022; revised on 16 October 2022; accepted on 19 October 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.16.1.1057

Abstract

Unprepared with a fragile digital infrastructures, and hurriedly tossed into the depth of the cyberspace in the Fourth and Fifth Industrial Revolutions (4IR and 5IR) by Covid-19 pandemic measures, of lockdown and needs for remote learning. The educational sector became the most vulnerable; with streams of cyber-attacks stalling virtual classes and compromising data integrity, of which the financial sector was not exempted, despite the evolvement of cyber insurance policy. The financial end users are aggravated and left at the mercy of internet fraudsters called "yahoo-yahoo" boys, coupled with hacking of SWIFT, crypto currency thefts, and Nations' Central Banks falling into cyber-attacks, thus leaving no unconquered space for cybercriminals, even as cyber literacy and security are siloed away under stand-alone arrangements despite the interconnectedness of the cyberspace. It was against this background, that this study leverages on Theory of Endogenous Growth Model to interrogate impact of cyberspace on the protection of critical national assets and infrastructures in Nigeria. The study deconstruct national assets into education and financial sectors to assess the existing impact. This study adopts qualitative research design using exploratory research design of publicly available archive documents. Empirical evidence from study revealed that cyberspace has expanded the virtual learning horizon while cyber attacks still remain on the minimal. Findings that emanate from this study revealed cyberspace has positively impacted on the Nigeria Financial sector through financial inclusion and transaction conveniences while the damaging effect of cyberattacks remained largely covered up. The study recommends that all players in the educational sector should invest widely in cybersecurity as days of imminent cyberattacks is on the horizon as seen evolving in developed clime. Study also recommend that government should firm up cyberspace policy, and inject collectivism into cyber security plans of sectors as an improvement on the present stand alone security by banks in Nigeria.

Keywords: Crypto currency; Cyber Insurance Policy; Cybersecurity; Digital Infrastructure

1. Introduction

The unmatchable pace of the fourth and fifth industrial revolutions came with disruptions. These disruptions quickens the interconnectedness of human, data and devices which ensure increase in convenience of device usage and expanse of activities on the cyberspace. These disruptions does not only challenge government sovereignty but fast track national security pressure, emanating from cyber criminals, to understand the impact, let alone control the disruptions, that societies could be subordinated to power of those who control new technologies, the digital systems and the criminal elements, who sees footage to occupy and ride it out (Susskind, 2018; World Wide Web Foundation, 2017). The digital infrastructure, interrogated by different critical assets cannot be ignored particularly, the educational and financial services sectors.

* Corresponding author: BILLE David Urbanus
Department of Security and Strategic Studies, Nasarawa State University, Keffi, Nigeria.

The interconnectedness of information systems trigger its universality, and this in essence accounted for what is wholly called the cyberspace. Interestingly, in second quarters of 2022 a total of 5.03 billion people representing 63.1 percent of the world's total population use the internet today compared to 1% of the world's population in 1995 (Internet Live Stats, 2022). The increase in internet usage has an uptick on cyber criminality. Activities of cybercriminal in the cyberspace ranges from theft and sale of corporate data, social engineering, Email and internet fraud, identity fraud from stolen personal identified information, theft of financial or card payment data, demands for money to prevent a threatened attack; called Cyberextortion, ransomware attacks, amongst others. The cyberspace is extensively rattled and aggravated limitlessly by cybercriminals due to poor cybersecurity education (International Telecommunication Union (ITU). (2012).

Globally, Italy and Israel trail behind India who suffered the highest volume of weekly attacks on their research and education facilities. Cyberattacks of malware and ransomware became aggravated on schools, virtual meetinngs and classes, universities, distance learning centres and research facilities, with loss of student coursework, school financial records amongst others (FBI's Cyber Division, 2021). The vulnerabilities could be seen in their online platforms and remote accessibility to large numbers of pupils and students, with often unprotected entry points for cybercriminals into the system. Cybercriminal endlessly exploited unpatched bugs or weak passwords, as well as unprotected remote endpoints to gain entrance. This pandemic propelled sector came into the cyberspace unprepared with less cybersecurity investments, despite it manages extensive and often sensitive information about students, faculty, researches and staff, whose exposure could have outreaching damages (Check Point, 2021; National Cyber Security Centre (NCSC), 2021).

The Covid-19 pandemic exposed the non-preparedness of the education sector worldwide, of which Nigeria was not excluded. The global lockdown precipitated uptick in remote learning through virtual classrooms, this further increases the vulnerability of the educational sector whose grasp of cyber security against cyberattacks was nothing commendable (Ben-David, 2021). While the increasing cyberspace undertakings in Nigeria, cannot be detached from data costs and different internet payment packages flaunted by telecommunication operatives (Techpoint, 2020), it is quite worrisome that despite the significant increase recorded in internet usage in Nigeria, a substantial proportion of the servers are not secured, and these accounted for the alarming rates of cybercrime in the country (Ibrahim, 2019; World Development Indicator (WDI), 2016).

Cybercrime in Nigeria does not only aggravate the financial sector endlessly, with individual at the mercy of internet fraudsters called "yahoo-yahoo" boys but also shows the desperate efforts of financial institutions to keep the hacking of plethora they are subjected to, away from the glare of the public (Lambo, 2022). As more people are lured by the appeals of money transfer Apps, working from home, and transacting from convenience point, more cybercriminals targets personally identifiable information (PII), which is leverage upon to execute account takeover fraud. A PII is a hot article of trade on the dark web which once surreptitiously taken, gives access to, online bank accounts, biometric, and driver license numbers (Federal Trade Commission, 2022). Another threatened financial service infrastructures outside the fiat money range, is the cryptocurrency whose operation's privacy is being infiltrated by cyberattacks (Sami, 2022).

Furthermore, the impregnability of crypto currency has been discounted with several cyber-attacks depleting hot wallets connected to the internet thus signaling the safety of Cold wallets due to being detached from internet. The operation secrecy shrouding cryptocurrency as envisaged by Satoshi Nakamoto is being shredded by the interconnectedness of cryptocurrency with the cyberspace. The Lazarus Group who are linked with crypto currency hacking and ties to North Korea's primary intelligence bureau, the Reconnaissance General Bureau, are largely fingered in the "WannaCry" ransomware attacks, the hacking of international banks and customer accounts and cyber-attacks on Sony Pictures in 2014. Such illicit funds through cyberattacks are allegedly used by North Korea for her Nuclear Ballistic program. The attention given by North Korea to children with knacks for mathematics could be seen as promoting cyber education (British Broadcasting Corporation (BBC), 2022).

Cybersecurity education when properly channeled did not only equip the population for shifts in labour demands but it adequately armed populace with requisite training and skills which is randomly unavailable in Nigeria and this signals unpreparedness. The abysmal disconnect of the educational system from kindergartens to preschool, primary school and post primary education to latch onto nuances from the 4IR and 5IR is not only concerning but worrisome. A well-structured and pursued curriculum in this order could help the education infrastructure to evolve a healthy cyberspace culture that could evolve a generation of cyber commandoes whose narratives can counter the criminal narratives displayed by the notorious yahoo-yahoo boys whose trends of cyberattacks extend beyond the developing clime and is unsettling even the US Federal Bureau of Intelligence (FBI) (Srikonda, 2022; Ratliff, 2021).

The Nigeria cyberspace witnessed cyberattacks from global hackvists during the #ENDSARS protest in Nigeria. The event witnessed Syrian Electronic Army (SEA) creating A DDOS attacks on selected website in solidarity to the youthful protesters on police brutality. Some notable public institutions websites were hacked and supports for the protest were emblazoned on compromised sites; Central Bank of Nigeria (CBN), Nigeria Communication Commission (NCC), Police Service Commission. All these done to the helplessness of the security agencies whose grasp of the cyberspace is quite limited. The helplessness could be seen in security agencies wariness in responding to the non-guerilla tactics adopted by protesters and their sponsors who equally leveraged on crypto currency as against the fiat money. While security agencies threaten protesters with arms and ammunitions rather than been on equal or advance footing on the cyberspace, the Central Bank went into closing down accounts of involving celebrity supporting and canvassing for the protest. This did not only constrict public civil space but unveil the poor cybersecurity policy drive of Nigeria (Mungadi *et al.,* 2021).

The absence of a pursued Cybersecurity Policy and Strategy which raises awareness and affect cyberculture, while closing up, sustaining and ensuring that international cyberspace initiatives are linked to a national strategy, is not only essential but should be seen aggressively pursued by all developing nations, of which Nigeria is not exempted. An informed Cybersecurity policy will not only scale up awareness level of users, keep users a step ahead of cybercriminals but will allow vulnerable corporate and government institutions to go beyond individualized cyber security measures (Trelix, 2022). Evolving a comprehensive approach via constant threat awareness, proactive measures that constantly anticipate risks, vulnerabilities and hedge against such unrelentlessly, will help to protect and ensure the safety of the cyberspace.

Interestingly, risks and vulnerabilities are endlessly being anticipated not only by cryptologist and Artificial Intelligence (AI) engineers, but Machine learning, quantum computing developers and deep learning engineers, committed to protecting the confidentiality, authenticity and integrity of data by anticipating risks, detect threats and react more quickly thus scaling up the resilience of a could be threatened system (Innovate Cybersecurity, 2022). The action plan to generalise such awareness level of cyberthreats, attacks and vulnerability could be seen in a cybersecurity policy or strategy. The thrust of a Cybersecurity strategy is the building of collaboration between stakeholders on information sharing and the creation of Public-Private Partnerships in improving the cybersecurity and resilience of national infrastructures and services within a secure computing environment (European Union Agency for Cybersecurity (ENISA, 2021).

The Nigeria's Cybercrime (Prohibition, Prevention, etc) Act 2015, well conceptualised on the paper in the order of what is obtainable in developed world is yet to be seen actively engaged in the services of all federal security agencies nor seen in the protection of her financial and education sectors. The cyberspace has gone beyond states' war capabilities, Cyber strategy is well woven around state and public Private partnership, with awareness level constantly scaled up and this is extremely missing in Nigeria cybersecurity policy. The concentric nature of the national security architecture which lacks flexibility to attend to a federal system (Maibashira, 2022; Afuzie, 2022), could be seen playing out on the national cybersecurity policy.

The significance of this study lies in its capabilities to stimulate discussion among researchers, practitioners, and policy makers interested in the impacts of cyberspace collaborations as against siloed individual cybersecurity of critical national assets, and to deepen the need for cyberspace awareness that constantly update cyber security architecture, particularly on the financial services and education sectors It is against all these background that this present study sets out to examine the impact of cyberspace on cybersecurity of critical national assets particularly the education and financial service sectors of the Nigeria economy.

In a bid to achieve the objective of this study, answers are provided to research questions below:

- What is the impact of cyber security on the education sector in Nigeria?
- How does cyber security impact on the financial sector in Nigeria?

2. Literature Review

2.1. Conceptual Framework

2.1.1. Education Sector and Cyberspace

The impact of the cyberspace could be seen from the fusion and interaction of technologies across the physical, biological, and digital domains, which etched out the 4IR and the 5IR from previous revolutions (Schwab, 2016). There is no gainsaying that poor cyberspace education has not been helpful both in latching Africa's manpower into the evolving industrial revolutions. Some jobs will disappear, others will grow and today's uncommon jobs will become commonplace, while the failure of government to inspire young people through an enabling platform is worrisome. Nations whose educational curriculum does not have embedded in it the competencies required for this changing world is at risk of being left behind.

The need to educate for critical thinking and problem-solving, creativity and innovation, collaboration and teamwork, communication and information literacy, right from kindergartens. Creativity and innovation among mathematics teachers, sharing ways teachers can maximise the resources at hand and the already available technologies which can be incorporated to better impart knowledge to learners. Africa's education system should be very intentional in ensuring that the requisite skills are integrated and this responsibility squarely falls on the government. Literacy of basic computer is generally missing at public schools while the private schools play lip services to same, not to mention inability of introducing pupils to computer coding literacy even in the said top flight schools.

The existence of these gaps constitute major constrains for the right entrepreneur mindsets needed for Start-up tech firms, rather criminality becomes the order of the few ones whose attentions are skewed toward cybercrime and internet fraudulent activities. Cyberspace education when properly ordered could evolve a generation of cyber commandoes who could be hired to counter the narratives of cybercriminal of hackers. Presently China has well over five million cyber commandoes actively involved both in the private and public space.

2.1.2. Financial Sector and the Cyberspace

After infiltrating the World's impregnable SWIFT financial system through the Bangladesh's central bank cyber heist in 2016. Cyber criminals are not just targeting consumers, staffers, providers, Central banks and financial sector but are massively consolidating by information sharing and service outsourcing. Streams of hacking into banks server has also heightened calls for banks to be held responsible for scam losses. The fundamental questions to be asked is whether banks have done everything they reasonably should to prevent these frauds and take action once scam occurred. Breaking such evolving dark web will be for a responsive government to facilitate threats information sharing across Nigeria's agencies and critical infrastructure, through a Computer Emergency Response Team (CERT).

A financial CERT offers specialised cyber security support services to the financial sector, including training, situation analysis, a platform for threat information sharing and cooperation, and incident response, for strengthening the financial sector's resilience against attacks, by proactively identifying threats and promoting protection, advancing preparedness, and collaborating with financial institutions worldwide. A web of agencies from ministry of Interior that houses NIMC; of national data, NSCDC; lead security agency for the protection of national Assets, NCC; host of all telecommunication operators, financial institutions, Fintech and Finsec companies, the Nigeria Police, EFCC, ICPC, DSS and the DIA must all be seen working together with the Nigeria's Electronic Fraud Forum to facilitate collaboration in mitigating and tackling fraud as well as restoring public confidence in card usage, electronic payments and cyber related activities.

2.1.3. Cyber Liability Insurance Policy

This is an insurance cover that safeguards organizations against financial losses, reputational and brand damage caused by cyber incidents, including data breaches and theft, system hacking, ransomware extortion payments and denial of service. The embryonic stage of this product in Nigeria is attested to by the absence of policies covering cyber liability in the financial statement of financial services or education services rendering institutions in Nigeria (Oaikhena, 2022; Tijani & Oloyede, 2020).

Interestingly, the Central Bank of Nigeria in her Risk Based Cybersecurity Framework provided that cyber-insurance coverage should be considered as part of security assurance program for Payment Service Providers. Same could not be said of any similar provisions in the Insurance Act 2003 nor its amendment. Most banks in fear of reputational damage or customer unguided panic withdrawal do sweep their cyberattacks away from the public knowledge while efforts for integrated efforts to secure the financial services industry is also at its nascent stage thus limiting collective approach and awareness

3. Factors Aggravating Cyberattacks in the Nigeria Cyberspace

3.1. Skimming and Key Pad Overlay

This is known as ATM skimming, commonly practiced by the insertion of a counterfeit reader into ATM machine that reads and stores all the information given on the magnetic strip on the card. The compromised personal identified data is later used by hackers for stealing money. Same goes for Key pad overlay, where Criminals install fake keypad over on the actual keypad to steal the PIN. Capturing people's PINs through a false keypad

3.2. Hidden Cameras

Another common way that criminals use to steal your money is by installing hidden cameras near ATM machines. These spy cameras are strategically fitted in a way to read your card PIN number. Since they are quite small in size, so are usually fitted near the keypad.

3.3. Pharming

This entails hackers modelling a replica site like the original whereby unsuspecting users unknowingly transact and pay via credit or debit cards, the card details are stored and later used to steal money from the unsuspecting users.

3.4. Near Field Technology

A Near Field Technology (NFT) affords payment to be effected for transaction, such that the users mobile phone is placed near or brought closer to waiters scanner. This emerging technology though tightly controlled in most countries, but its usage transmits its vulnerability. European law requires NFT payments to go to business entities. This means that a fraudster would have to create one to access NFT payments. The limit on how much can be paid through NFT payments is €20. This minimizes the damage a scammer can do if he gets his/her hands on your information.

3.5. Cloned SIM Card

A trending hacking means occurs when soft targets cellphone users in tier-II and tier-III towns are left with missed calls. These users, not with the least clue about the possibility of a SIM card being cloned only by returning a missed call until they get alerts of money being withdrawn from their accounts or receiving huge telephone bills for downloading information from the Internet.

3.6. Free Wi Fi

Malicious hackers also leverage through open wireless access points, enticing unsuspecting individual who connect to for free, and start browsing the Internet, not knowing it was specially configured by hackers with the purpose to harvest confidential information

3.7. Spoofed Apps

This is mostly executed by tricking users with fake banking Apps done through spoofed banking app. A malware programmer creates a perfect replica of a bank's app and uploads it to third-party websites. Once you've downloaded the app, you enter your username and password into it, which is then sent to the hacker.

4. Empirical Review

4.1. Cybersecurity and Education Sector in Nigeria

Mungadi *et al.* (2021) employed routine activity theory to investigate effect of the nationwide #EndSARS cyber warfare protest on Nigeria's critical national asset and infrastructures. The study engaged purposive sampling techniques and regression for data analysis. Results from study revealed that the protest's unconventional cyberwarfare approach confirms that cyberwarfare knowledge is still an unfamiliar terrain even to the law enforcement agencies shallow grasp of cyberwarfare. The study submitted that, there exist urgent need for cyberwarfare empowerment particularly for the Nigeria Security and Civil Defence Corps who is the lead agency in the protection of Critical National Assets, as cyberthreats is no longer in the realm of imagination but real. Study was limited to #EndSARS protest while this study review financial service and educational sectors.

Ndagi and Salihu (2019) adopted qualitative research design to amplify embedded prospect and challenges of the fourth industrial revolution for Africa. The study relied on extant literature and related publications. Results from the study showed that disrupting technologies are causing the loss of low-skilled routine jobs in the manufacturing sector hence the need for a rethink by Africa. Study was limited to the manufacturing sector while this study captures the impact of cyberattacks on the cybersecurity of the banking and educational sectors

Kayembe and Nel (2019) engaged desktop research study to investigate opportunities and challenges in the fourth industrial revolution for education in South Africa. The study engaged unobtrusive research techniques of both conceptual and documentary analysis on related materials, publications and government report. Findings of the study showed that there exist numbers of challenges; infrastructural deficit, insufficient funding and requisite skills for South Africa to attain 4IR. Study submitted implications of the 4IR for education entails a new digital approach to teaching and learning, R&D, teacher development, pedagogical adaptation, and skills development which are grossly inadequate. The study was limited to educational sector of South Africa while the present studies considers financial sectors, communication sectors, transportation sectors and comparative studies of Africa regional studies.

Kennedy (2019) thematically reviewed what schools in South Africa need to know about cyberspace awareness and the Fourth Industrial Revolution. Study engaged government policies, publications, occurring observations in South Africa. Study submitted that technologies using social robots to impart on special needs students, usage of 3D printers also assist to create new and innovative teaching even as 3D printing has turned design education on its head. Study opine that virtual Reality has been shown to work throughout different levels of schooling, heightening subject engagement, enlivening teaching and facilitating learning and linking studies with the real world. Study establish that the key skills and values are creativity, critical thinking and problem solving. Study was limited to impact of 4IR on education of which present studies intends to go beyond through financial sectors.

Badran (2019) employed labor market panel data to investigate the nexus between technological change and the labor market in Egypt. The study engaged ordinary least square in data analysis. Findings from study showed that that there exist evidence of impact of technological change on employment in the years 2006 and 2012 causing job polarization in the labor market as revealed in the first approach. The study analyzes the impact technological change has on the labor market. The study captures the education sector while this study will consider the financial sector also.

4.2. Cybersecurity and Financial Sector in Nigeria

Ndung'u and Signé (2020) interrogated digital disruption on the financial services sector from core banking functions to regulatory impact in South Africa. The study engaged qualitative research design. The study submitted that the shift towards automation enable vast opportunities for improving efficiency but also impacts financial institutions' skill requirements, potentially entrenching the existing "low-skill low-pay" and "high-skill high-pay" labour divide. More broadly, digitization is enabling entrepreneurs and businesses to rethink business models that are more impactful, sustainable, and connected to other sectors of the economy of which the government is also migrating to online platforms conveniently. Study did not capture the education sector which this study considers.

Oaikhena (2022) interrogated the embryonic stage of cyber liability insurance in Nigeria in a qualitative study. Study submitted that there is the need to take a more proactive approach to cyber-security now that cyber insurance brokers and lawyers start to serve as risk advisors and partner to business whose large chunk of operations depends on technology, hence exposure to cyber risk heightened. In a similar study Tijani and Oloyede (2020), investigated cyber Insurance in Nigeria and her risk hedging capabilities in an increasingly threatened landscape. Study corroborated the nascent stage of cyber liability in Nigeria such that finding revealed that top ten insurance firm had no provision in their financial statement for cyber liability policy. Studies in this regard was limited to financial service sector while this study extends to the education sector.

Mungadi *et al.* (2021) investigated the vulnerability of Nigeria's critical national asset and infrastructures during the nationwide Endsars cyber warfare protest. The study employed triangulation research design with purposive and snowballing sampling techniques and regression for data analysis. Findings from the study showed that the nation's information and financial infrastructures were extensively overwhelmed during the protest to no avail with both NARSDA nor NITDA helpless in rescuing the penetration of the hackvisit. Study submitted that more need to be done in the protection of CNAI as cyberwarfare is beyond rhetoric. Study did not consider cybersecurity policy nor legal framework but limited to critical national assets of which this present study will consider not only at State level but within the. African regional

Okifo and Igbunu (2015) interrogated the economic benefits and challenges of the adoption of E-payment system in Nigeria. The study was an exploratory study with reliance on extant literature. Study submitted that e-payment is faced with lack of uniform platform being, operated by the banks, lack of adequate infrastructure and issues of security. The study query the security and privacy being offered across the networks even as consumers became more aware of their privacy and security. Study though on e-payment using internet did not explore the cyberspace and cyber attack as related to the financial sector nor the education sector which this study does.

Maitanmi *et al*. (2013) investigated the impact of cybercrimes on Nigeria economy by probing the level of awareness of individuals on cybercrimes and its impact on Nigerian economy. Study engaged survey research design with administered questionnaire. Analysis showed that pornography, software piracy, and cracking are among others prevalent cybercrimes in Nigeria. Study was on the economy with no focus education and financial sector which this study captures in order to arrive at a robust conclusion

5. Theoretical Framework

5.1. The Endogenous Growth Model

Endogenous growth model postulated by Romer (1990) has its thrust that, the key drivers of growth revolve around ideas generation and information dissemination. The massive growth and utilization of internet in recent years have strongly impacted on interconnectedness of systems across divides giving spikes to innovation, production and economic growth through the adoption of new technologies, cheaper information dissemination, development of new products and services and the promotion of new business models (Benhabib & Spiegel, 2005). The Internet has gradually become the central pivot of the digital economy as it supports a substantial portion of the world's economic and social activities serving as an active catalyst for technology and innovation, enhancing the social wellbeing and economic growth of the nation. The loss of wars as seen between Russia and Ukraine with Google disconnecting her goggle map services from the reach of the Russian Army in support of a free Ukraine (Mungadi *et al.*, 2022).

The internet is fundamentally designed to be open and global hence making the facility to serve as the hub for technological innovation and economic growth and development. The internet is also fast emerging as a tool of sanctioning belligerent nations as seen when social media; twitter, whatsapp, Google, yahoo all yanked off from Russia Armed Forces from their services (Mungadi *et al.*, 2022). The support from the internet enables firms to take advantage of trans-border data flows across nations to monitor the production value-chain across different areas (Salahuddin & Gow, 2016). Hackers in the dark web world freely exchange ideas for status recognition and for economic gains, reaching out to freely impart cyber knowledge and provide hackable clients to their new recruits. Whereas, targetable corporate institutions are standing alone with siloed cybersecurity whose protection infrastructure still experience colossal loss to cybercriminal from the dark beyond.

6. Methodology

This study engages exploratory research design to examine impact of cyberspace on the cybersecurity of critical national assets infrastructures of education and financial sectors in Nigeria. The study relies solely on secondary data from available archive documents. The research is conducted by examining literature concerning the cyberspace and critical national assets alongside the fourth and fifth industrial revolutions. The literature was obtained through searches in publicly available material. Literature from non-serial publications, official reports, and conferences has been included particularly if they have been cited by other references in term of national security architecture, criminology, criminal justice system and human security.

7. Discussion

Reviews garnered on research question one, on the extent to which cyberspace influences the education sector in Nigeria? Empirical evidence opines that Nigeria education sector under the impact of Cyberspace has expanded the virtual learning horizon, working remotely from homes, presentations of dissertation defence at all stages of presentations by postgraduates but largely untapped particularly by public learning institutions while cyberattacks remain on the minimal with little or no investment in cybersecurity to protect the nascent fragile cyberspace of the education sector. The finding is in tandem with the findings in the previous works of Mungadi *et al*. (2021); Ndagi and Salihu, (2019); Kayembe and Nel, (2019); Kennedy, (2019); Badran (2019) who found that there exist a significant impact of the Cyberspace on the education sector while cybersecurity is not yet aggravated within the Nigeria digital infrastructure whose cybersecurity investment is still at its nascent stage.

The result elicited from research question two, from logical findings and literature review; as to what extent has cyberspace aggravates the financial service sector in Nigeria? Evidence abound that the Cyberspace has positively impacted on the Nigeria Financial services sector through financial inclusion expansion and transactions conveniences while the damaging effect of cyberattacks remained largely covered up from public view with no provision for cyber insurance liability policy. Individual institutions siloed away within their cybersecurity provision is not curtailing the aggravated cybercriminal attacks on financial institutions digital infrastructure. Such that cybersecurity should be complimented by cyber insurance liability policy and products. This finding is consistent with the findings in the previous work of Ndung'u and Signé (2020); Oaikhena (2022); Mungadi *et al*. (2021); Okifo and Igbunu (2015); Maitanmi *et al*. (2013).

8. Conclusion

The study concludes that since the cyberspace belongs to nobody but of everybody, international collaboration is necessary and urgent in countering the dark and criminal world of hackers and hackvists, as the independent nature of individual governments, financial firms, institutions of learnings and tech companies simply aggravate their cyberattacks vulnerability which cannot effectively protect against cyberthreats by working individually. Hence the need for collectivism when approaching cybersecurity for the vulnerable digital infrastructure. Some initiatives to protect financial institutions are not only individually fragmented and siloed away but are duplicated thereby increasing transaction costs.

Several of these initiatives are mature enough to be shared, better coordinated, and further internationalized since reduction in fragmentation will free up capacity to tackle the extensive outreaches of hackers. While the Nigeria Government should build an effective cyberdomestic relationships among financial authorities, law enforcement, industries, diplomats, other relevant government actors, and industry. As existing fragmentation hampers international cooperation and weakens the international system's collective resilience, recovery, and response capabilities

Recommendation

Based on the above submissions,

- The study recommends that all players in the educational sector should invest widely in cybersecurity as days of imminent cyberattacks is on the horizon as seen evolving in developed clime. Maintaining proper cybersecurity hygiene within a unified digital infrastructure.
- The CBN should look beyond individualism to strengthen cybersecurity by sharing information on threats and by creating financial computer emergency response teams (FinCERTs) as seen in Israel. While the Federal Government should firm up cyberspace policy, incorporate cyber liability policy such that the Central Bank of Nigeria should project collectivism of cybersecurity into the national digital infrastructure as an improvement on the present standalone cybersecurity by financial service providers in Nigeria.

Compliance with ethical standards

Acknowledgments

Sincere appreciation goes to Prof Ochefu (NSUK), Prof Akinwumi (VC FUL), Prof Zamani (NSUK) and Dr Yusuf for the template given for this academic exercise.

References

[1] Badran, M. F. (2019). Technological Change and its Impact on the Labor Market in Egypt, 2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, Egypt, 18th-21st February., International Telecommunications Society (ITS), Calgary

[2] Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber Security in Financial Sector Development Challenges and potential solutions for financial inclusion. Retrieved from

https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf

[3] Benhabib, J., & Spiegel, M. (2005). Human Capital and Technology Diffusion. In: Handbook of Economic Growth, Volume 1A, P. Aghion and S.N. Durlauf (eds.), 935-966. Amsterdam: Elsevier

[4] Ben-David, R. (August 21, 2021). Education sector sees 29% global increase in cyberattacks, Check Point reports. Times of Israel. Retrieved from https://www.timesofisrael.com/education-sector-sees-29-global-increase-in-cyberattacks-check-point-reports/

[5] British Broadcasting Corporation (BBC). (January14, 2022). North Korea hackers stole $400m of cryptocurrency in 2021. BBC NEWS. Retrieved from https://www.bbc.com/news/business-59990477

[6] Checkpoint. (2021). Providing cyber security professionals and C-Level executives a detailed analysis of key cyber trends, statistics and advice on how to prevent fifth generation cyberattacks. Cyber Security Report 2021. Checkpoint. Retrieved from https://www.checkpoint.com/pages/cyber-security-report-2021/

[7] European Union Agency for Cybersecurity (ENISA). (2021). National Cybersecurity Strategies. Enisa Europa. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[8] Federal Trade Commission. (February 22, 2022). New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

[9] Ibrahim, U. (2019). The impact of cybercrime on the Nigerian economy and banking system. NDIC-Quarterly, 34(12). Retrieved from https://ndic.gov.ng/wp-content/uploads/2020/08

[10] Innovate Cybersecurity (August 30, 2022). Artificial Intelligence Is Making a Massive Impact—Just Not in Cybersecurity. Retrieved from https://innovatecybersecurity.com/news/artificial-intelligence-is-making-a-massive-impact-just-not-in-cybersecurity/

[11] Internet Live Stats. (2017). Available at www.internetlivestats.com/internet-users/.

[12] International Telecommunication Union (ITU). (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response. Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[13] Kayembe, C., & Nel, D. (2019). Challenges and opportunities for education in the fourth industrial revolution. African Journal of Public Affairs, 11(3), 79-94.

[14] Kennedy, K. (2019). Another Industrial Revolution: What schools need to know. Kagiso Trust and the University of Johannesburg.

[15] Lambo, D. (September 21, 2022). Fraudsters hack bank, transfer N523m to 225 accounts. The Punch News. Retrieved from https://punchng.com/fraudsters-hack-bank-transfer-n523m-to-225-accounts/

[16] MaiBasira, A. H. (July 13, 2022). Nigeria: Reforming the security architecture. This Day. Retrieved from https://www.thisdaylive.com/index.php/2021/12/29/nigeria-reforming-the-security-architecture/

[17] Maitanmi, O., Ogunlere, S., Ayinde, S., & Adekunle, Y. (2013). Impact of cybercrimes on Nigerian economy. The International Journal of Engineering and Science, 2(4), 45-51.

[18] Mungadi, D. D., Kana, A. A., Yusuf, A. U., Owa, F. T., Abubakar, I. A., & Onibiyo, E. R. (2021). Endsars cyber warfare protest and critical national asset and infrastructures in Nigeria. Infokara Research, 10(3), 194-208.

[19] National Cyber Security Centre (NCSC). (2021). Making the UK the safest place to live and work online. NCSC Annual Review. Retrieved from https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021

[20] Ndagi, A., & Salihu, A. A. (2019). Fourth industrial revolution: prospects and challenges for Africa. Dutse Journal of Economics and Development Studies, 6(1), 189-198.

[21] Ndung'u, N., & Signé, L. (2020). The Fourth Industrial Revolution and digitization will transform Africa into a global powerhouse: Foresight Africa In Capturing The Fourth Industrial Revolution A regional and national agenda

[22] Okifo J., & Igbunu, R. (2015). Electronic payment system in Nigeria: its economic benefits and challenges. Journal of Education and Practice, 6(16), 56-64.

[23] Oaikhena, V. (January 25, 2022). Cyberinsurance: The State of Nimbleness in Nigeria. Mondaq. Retrieved from https://www.mondaq.com/nigeria/insurance-laws-and-products/1153878/cyberinsurance-the-state-of-nimbleness-in-nigeria

[24] Ratliff, E. (June 30, 2021). The Fall Of The Billionaire Gucci Master. Bloomberg. Retrieved from https://www.bloomberg.com/features/2021-hushpuppi-gucci-influencer/

[25] Romer, P. M. (1986). Increasing returns and long-run growth, Journal of Political Economy, 94, 1002-1037.

[26] Salahuddin, M., & Gow, J. (2016). The effects of internet usage, financial development and trade openness on economic growth in South Africa: a time series analysis. Telematics Inform, 33(4), 1141-1154 https://doi.org/10.1016/j.tele.2015.11.006

[27] Sami, T. (August 26, 2022). Cyber attacks: Crypto platforms lose $44bn. Punch Newspaper. https://punchng.com/cyber-attacks-crypto-platforms-lose-44bn/ Schwab, K. (2016). The Fourth Industrial Revolution. Geneva: World Economic Forum

[28] Srikonda, S. (March 30, 2022). Key Nigerian conspirator arrested in Mahesh bank hacking case. Retrieved from https://www.siasat.com/3-nigerians-22-indians-arrested-in-mahesh-bank-hacking-case-2299326/

[29] Susskind, J. (2018). Future Politics. Living Together in a World Transformed by Tech. Oxford: Oxford University Press

[30] Techpoint. (June 23, 2020). The cost of Internet data in Nigeria is increasing, but it's not really obvious. Techpoint. Retrieved from https://techpoint.africa/2020/06/23/internet-data-nigeria-increased

[31] Tijani, R., & Oloyede, R. (October 1, 2020). Cyber Insurance in Nigeria: Risk Hedging in an Increasing Threat Landscape. African Academic Network on Internet Policy. Retrieved from https://aanoip.org/cyber-insurance-in-nigeria-risk-hedging-in-an-increasing-threat-landscape/

[32] Trelix. (2022). How Cybersecurity Policies and Procedures Protect Against Cyberattacks. Trelix. Retrieved from https://www.trellix.com/en-us/securityawareness/cybersecurity/cybersecurity-policies.html

[33] World Development Indicator (WDI). (2016). International Bank for Reconstruction and Development/The World Bank; Washington D.C, USA. https://www.diplomatie.gouv.fr/

[34] IMG/pdf/paris_call_cyber_cle443433.pdfhttps://www.weforum.org/agenda/2019/01/addressing-the-growing-cybersecurityskills-gap/

[35] World Wide Web Foundation. (2017). Artificial Intelligence. The Road Ahead in Low and Middle-Income Countries. Washington DC.