Global Academic and Scientific Journal of Multidisciplinary Studies (GASJMS)

Volume 3 | Issue 8, 2025 Journal Homepage: https://gaspublishers.com/gasjms/ ISSN: 2583-8970
Email: gaspublishers@gmail.com

Impact of Cybersecurity on Digital Economy in Southeast Nigeria

Bala, Iranyang Shamaki[1]; Anthony, Shalon[2] & Ofodogu, Eucheria Uche[3]

[1]Department of Political Science, Federal University Wukari, Taraba State
[2]Excel Model Secondary School, Wukari, Taraba State
[3]Department of Political Science, Federal University Wukari, Taraba State

Received: *20.07.2025* | ***Accepted:*** *23.08.2025* | ***Published:*** *26.08.2025*

***Corresponding Author:** Bala, Iranyang Shamaki

DOI: *10.5281/zenodo.16950036*

Abstract **Review Article**

The dominance of cyberspace in the 21st century, with the adoption of advanced technologies, has led to a significant economic shift towards digital platforms. The South East region of Nigeria is gradually advancing in the adoption of the digital economy. The impact of cybersecurity on the advancement of the digital economy cannot be underscored. This paper investigates the state of the digital economy in South East Nigeria using the pillars of the digital economy as a yardstick of evaluation, identifying the threats and challenges of cybersecurity on the digital economy in the region, which include data breaches, cyber-attacks, cybercrime, and infrastructure challenges, among others. The study analyses the impact of cybersecurity on the digital economy of the region, which includes: protection of information, trust and confidence, financial loss, reputational damage, etc. The research employs an ex post facto research design supplemented by secondary sources of data. The study integrates public good theory as the theoretical framework for this study. The research proposes strategies to enhance cybersecurity, which include the provision of advanced cyber infrastructure, collaboration among the government and stakeholders.

Keywords: Cyberspace, Digital Economy, South East Nigeria, Cybersecurity, Data Breaches, Cyber-Attacks, Cybercrime, Infrastructure Challenges, Information Protection, Trust, Confidence, Financial Loss, Reputational Damage, Ex Post Facto Research Design, Public Good Theory, Cyber Infrastructure, Government Collaboration, Stakeholders.

INTRODUCTION

In the digital economy ecosystem, cyberspace plays a pivotal role as a unifying factor, facilitating online product and service offerings, consumer engagement, and market expansion for firms. This has prompted the global economy to adopt technologies, resulting in increased productivity and economic growth. In the words of Ujah-Ogbuagu (2023), the digital economy is the oil of the 21st century, promoting economic growth, innovation, and job creation, among others. However, it also presents security risks that can threaten business, organization, and national defense through security gaps in its digital network. It essential to improve cybersecurity to mitigate cyber threats and risk, cybersecurity is no longer about preventing attack; it is the conerstone of digital economy.

The United States, the Netherlands, Singapore, Denmark, and Switzerland were identified as the top five countries in the ranking of the rise of the digital economy, according to the World Digital Competitiveness ranking of 2023 (IMD, 2023). These countries are also targets of cyberattacks. Cyberattacks across the globe, according to the Global Security Index Report (2018), focus on five sectors: government, financial services, transportation, manufacturing, and health care. These sectors are expected to cause significant damage and potentially incur substantial economic losses (Cybersecurity Ventures, 2020).

With the penetration of the internet and mobile phones in Nigeria, Nigeria ranked eleventh globally according to the Nigeria Communications Commission (NCC) (Izuaka, 2023). Nigeria's adoption of the digital economy led to the establishment of the Federal Ministry of Communications and Digital Economy in 2019, tasked with spearheading the country's adoption and exploration of digital technologies as a key driver for transforming the economy. With the adoption of the digital economy, which places significant reliance on cyberspace, come the impacts, threats, and challenges of cybersecurity. According to Cyber Security Experts of Nigeria (CSEAN), Nigeria experienced a 7% increase in cyber-attacks on individuals and corporate bodies during the first half of 2023. 71% of Nigerian organizations were victims of cyber-attack (Leyden, 2024). These threats do not respect national

boundaries and have no limitations on who the threat actors can target.

This paper focuses on the South-East region of Nigeria. With the emergence of the Internet of Things (IoT), artificial intelligence, and advanced technology, it is crucial to explore and navigate the digital economy to maximize the social and economic impact in the Southeast region, given its reputation for commercial activities. Knowing well that the continuous advancement of the digital economy lies in cyberspace, it is a truism to ignore the role of cybersecurity, which is like a two-edged sword; it either transforms or destroys. It is important to research this issue and make practical applications in order to promote and enhance the transformation of the current economy into a robust digital one. It is crucial to adopt strict and effective cybersecurity controls. According to the International Telecommunication Union, the United States of America is rated the highest with the best cybersecurity measures; other countries include Canada, Australia, Malaysia, and Oman (ITU, 2020). With meaningful and reliable measures and implementation of cybersecurity, the region's digital economy will make significant headway and be ranked high in terms of digital economy growth and development.

The objectives of this paper are to study the impact of cybersecurity and the digital economy in South East Nigeria. However, the specific objectives of the research are to;

- Evaluate the state of the digital economy in the South East region
- Identify threats and challenges of cybersecurity in the digital economy
- Analyse the impacts of cybersecurity on the digital economy
- Propose strategies to enhance cybersecurity

METHODOLOGY

This research employs an Ex post facto research design, also known as 'after the fact research', which is a non-experimental research method where researchers investigate existing conditions or events to explore potential cause and effect relationships. This research analysis utilizes secondary data from literature reviews and narrative text analysis to address the research objectives.

Conceptual Definition

Cybersecurity Concept

The term "cybersecurity" is the collection of technologies, procedures, practices, responses, and mitigation mechanisms meant to protect networks, computers, programs, and data against attack, damage, or unauthorized access to preserve confidentiality, integrity, and availability (Public Safety Canada, 2014). Cybersecurity refers to preventing cyber-attacks, which include malware infections, phishing scams, hacking, and denial-of-service attacks. Effective cybersecurity minimizes the impact of cyber threats on organizations and individuals (UNCTAD, 2021). ISACA (2015) defined cybersecurity as the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems. Cybersecurity is a form of defense that involves using various technologies and techniques to protect computer systems, networks, and data from cyberattacks and other cyber threats (Hunker, 2013).

Therefore, cybersecurity involves the use of advanced technology to protect an organization's data, assets, and secrecy in cyberspace. Cybersecurity deals with the protection of cyberspace, actors, and assets.

Cybersecurity and the 5th Industrial Revolution

The world is on the cusp of a new era—the 5th Industrial Revolution—driven by rapidly evolving technological advancements. Hence, cybersecurity has become more important than ever. Given the rapid advancement of technologies, cybersecurity can truly be a game-changer in this new business paradigm.

Cybersecurity is not just about safeguarding data or networks; it is about protecting the very foundation of Industry 5.0. According to **Pranjal Sharma's** book, '**The Next New: Navigating the 5th Industrial Revolution'**, the 5th IR signifies the convergence of technologies like artificial intelligence, the Internet of Things (IoT), blockchain, and biotechnology. It is transforming how we live, work, and interact with the world around us.

Digital Economy

The term "digital economy" describes new forms of business, as well as new markets, products, and services, particularly those that are predicated on the use of digital technologies as an essential component of core corporate infrastructure. (Erondu & Erondu, 2023). Nguyen (2023) defined the digital economy as" the use of information technology to create, adapt, market, and consume goods and services that are based on the use of information technology, in order to make money. Digital economy refers to economic activities related to the use of digital technology, such as the internet, computers, and mobile devices, to conduct business (Westerman, Bonnet, & McAfee, 2014).

The digital economy enables businesses to reach global consumers, increase revenue, and enable customers to buy goods and services from anywhere, anytime. It is based on several components, including technological infrastructure, hardware, software, and networks, as well as digital mechanisms through which business and economic activities are conducted, including e-commerce and electronic transactions made entirely on the Internet (Freijat, 2023).

According to Juneja, Goswami, and Mondal (2024), Ekpeke (2024), there are pillars of the Digital Economy. This pillar encompasses a wide range of services delivered digitally.

- Digital services; Online platforms for entertainment (streaming services, online gaming), digital content creation and distribution (e-books, digital music, podcasts), Online advertising, cloud computing,

Software-as-a-service (SaaS), and various online platforms and marketplaces that facilitate service provision.

- Digital infrastructure: advanced infrastructure such as telecommunications networks, broadband internet access, data centers, and cloud computing services.
- Digital communication; It includes email, instant messaging, video conferencing, virtual meetings, project management tools, and collaborative workspaces.
- Digital finance; It includes online banking, mobile payment platforms, digital currencies (such as Bitcoin), crowdfunding, robot advisors, and peer-to-peer lending.
- Data and analytics; the digital economy utilizes vast data for data collection, analysis, and utilization, providing valuable insights, enhancing customer experiences, and driving innovation.
- Digital literary skills and education
- E-government and public service
- Digital entrepreneurship and innovation

Related Works

Some scholars have researched different areas of the Digital economy and cybersecurity. Ujah-Ogbuagu (2023) conducted research assessing the state of digital economy development in Nigeria. Adopting a mixed method of data collection, the author highlighted the need for Nigeria to leverage digital technology, as the government should be involved by setting up a monitoring mechanism, improving digital infrastructure, and providing grants for research in digital technology, among others. Juneja, Goswami, and Mondal (2024) asserted the importance of trust and confidence of individuals and organizations in the digital economy. Erondu and Erondu (2023) and Kala (2023) analyzed the importance of securing cyberspace. The authors highlighted cybersecurity threats like malware, information theft, and fraud. The critical role of cybersecurity in the global economy cannot be overstated; a breach in cybersecurity can have severe implications for the economy. Therefore, it is crucial to adopt security measures and policies to ensure the integrity of the information system. The research emphasizes the need for proactive measures to protect digital assets. In the domain of cybersecurity, the dynamic interplay between attackers and defenders can be aptly likened to a game of cat and mouse. Attackers persistently scour for system vulnerabilities, while defenders diligently strive to identify and remediate these weaknesses preemptively (Adewopo, Azumah, Yakubu, Gyami, Ozer, and Eldayed, 2024). These increased cyber threats in cyberspace could cause socio-economic damage. Ukuoma, Williams, and Choji (2022) suggest the need for urgent response by states and governments to gather resources against cyber threats. Thus, there is a need for international cooperation among states.

Spremić and Šimunic (2018) stated that cybersecurity activities should no longer be solely the responsibility of IT departments or assigned individuals (CISOs or similar), but institution-wide efforts with all employees engaged. As digital technologies are integrated into business strategies, the same approach should be applied to cybersecurity. According to Teoh and Mahmood (2017), nations require a national cybersecurity strategy (NCCS) to enhance cybersecurity, mitigate cyber risks, and protect against attacks, ultimately fostering success in the digital economy. Kademi (2018) identifies and discusses crucial concerns within the Nigerian National Cyber Security Strategy (NCCS) and proposes measures to strengthen it, which include enhancing institutional adjustments and fostering collaboration across levels.

However, there are still gap that needs to be addressed. There is a scarcity of research on cybersecurity and the digital economy focusing on the Southeast region.

Public Good Theory: Theoretical Framework

The theoretical framework for this research is Public goods theory. Nobel laureate Paul Samuelson popularized public good theory. The theory purports that public goods are goods or services that are non-rivalrous (consumption of the good by one actor does not result in the reduction of the overall availability) and non-excludable (the practical impossibility of excluding any actor from consuming the good). (Samuelson, 1954).

The assumptions of Public Good Theory are;

- Non-excludability: The theory assumes that all individuals benefit from the good and none is excluded (Samuelson, 1954).
- Non-rivalrous Consumption: The consumption of a public good by one individual does not reduce its availability to others (Samuelson, 1954).
- Free-Rider Problem: Individuals or organizations may opt not to contribute to public good provision, expecting others to bear the cost while still benefiting from it (Samuelson, 1954; Boyer & Butler, 2005).
- Collective Action: The theory assumes that the provision of public goods requires collective action and cooperation among individuals, organizations, or states (Samuelson, 1954)
- Government Intervention: The theory suggests that government intervention, such as regulations, funding, etc., is often necessary to ensure the provision of public goods. (Olson, 1965; Kindleberger, 1981)
- Global Nature of Public Goods: the need for international cooperation and coordination to effectively manage public goods and provide them, as their benefits and challenges transcend national borders (Keohane, 1984)
- Marginal Cost of Provision: The theory assumes that the marginal cost of providing the good to an additional individual is zero or very low.

Digital economy and cybersecurity are public goods that are consumed by all and beneficial to individuals, firms, and government for online business, ensuring the security and integrity of services like e-commerce and banking, thereby enhancing user confidence and promoting greater participation

in the digital economy. Cybersecurity is a public good, but it faces challenges like the free-rider problem, where individuals or organizations benefit from others' cybersecurity measures without contributing themselves. This issue is prevalent in the region, where small and medium businesses do not invest in advanced cybersecurity measures, leading to underinvestment and vulnerability to cyber threats. This reliance makes the entire digital economy vulnerable to cyber threats. Cyberspace has no limitations or boundaries and has united the world into a global community. Cybersecurity is a public good and has a significant impact on the growth of the digital economy. It is a necessity for collective actions by governments, agencies, international partners, and firms, among others. Public good theory assumes the marginal cost of providing the good to an additional individual is low (Gordon & Loeb, 2002)

The State of the Digital Economy in South East Nigeria

South East states, Anambra, Enugu, Abia, Imo, and Ebonyi, have shown significant progress in digital adoption. We will evaluate the state of the digital economy in the region using the pillars of the digital economy as a yardstick of measurement.

The digital economy in South East Nigeria has experienced significant growth, with mobile phone subscribers increasing from 10 million in 2010 to over 50 million in 2020, mainly due to active internet users (NCC, 2020). South East Nigeria is making strides in digital infrastructure, with investments in broadband and the introduction of 5G services by Telcos. Onwuka (2024) reported that the Anambra state government introduced the pilot phase of free public wifi known as Solution wifi. However, challenges like the absence of high-speed fiber internet in the region persist in rural areas, affecting the usability and effectiveness of digital services (TechEconomy, 2023).

Digital platforms such as Jumia and Konga, which facilitate e-commerce, are highly favorable to small and medium-sized businesses as they expand their consumer base and streamline their operations. Social media plays an important role in marketing and interaction with customers. There are also several e-commerce platforms in the Southeast region, which include: MadeInAba.com.ng, Proudlyanambra.com, Zuwanu, Ideas, ESOM, Agrobond, among others (Osamuyi, 2016; Nwankwo, 2024). Nwankwo (2023) asserted that E-commerce is in its infancy stage; the use of e-commerce in the region is yet to be fully utilized, as both physical goods and cash still dominate the market.

Digital financial services, including fintech like Flutterwave and Paystack, are expanding in South East Nigeria, reducing reliance on traditional banking systems and providing secure, convenient transactions to the unbanked population, with a 30% growth in 2020. There are also financial services based in the region, which include Switch Wallet and XEND, among others.

Through online portals for tax payments, company registrations, and public service information, e-government and public services efforts are improving governance and service delivery. In Anambra state, there is an establishment of an automated budget system, the introduction of GIS services in land management services, and the issuance of Anambra E-ID cards for public servants (TechEconomy, 2023)

Digital entrepreneurship and innovation in South East Nigeria are thriving, thanks to tech hubs and incubators like the Genesys Tech Hub in Enugu state, RAD5 Tech Hub, Aba in Abia state, Dev Amplify Hub, Awka in Anambra state, Testrogen Hub, Abakiliki in Ebonyi state, and Oluaka Institute in Imo state. These hubs offer resources, mentorship, and networking opportunities for startups, contributing to the region's economic growth. (Nsekpong, 2022). These tech hubs and universities offer education and digital skills like computer science, ICT, and other related disciplines. Thus, improving digital education skills in the region.

The Threats and Challenges of Cybersecurity

- **Cyber Attacks**: Cyber attacks, such as phishing scams, social engineering attacks, and ransomware and malware, are increasing in frequency. These attacks exploit digital system vulnerabilities and human factors to gain unauthorized access to sensitive information and financial resources (Ladipo, 2022; Kala, 2023). The National Cyber Threat Forecast 2024 from the Cyber Security Experts of Nigeria (CSEAN) projected the increase of these attacks affecting both public and private sectors (Leyden, 2024). According to Business Day (2022), cybersecurity experts reported that 43% cyber-attacks target small business and 60% falls victim.

- **Cybersecurity infrastructure;** the lack of advanced software and infrastructure by states, firms has made it vulnerable to attacks (Leyden, 2024). Most firms and small businesses fail to upgrade their cybersecurity and relied on the use of outdated system, these make them prone to threats and vulnerabilities.

- **Infrastructure Challenges;** There is poor Internet connectivity in the region, as confirmed by a report by NBS (2021), making it difficult to do business. Another infrastructure challenge is the frequent power outages in the Southeast region, which makes it difficult for businesses to operate efficiently, leading to financial losses and decreased productivity (Umeh, 2022).

- **Cybercrime**: Cybercrime refers to the activities of criminals conducted via the Internet (Goyal & Bhat, 2023). It has been reported that cybercrime assumes frightening dimensions in the Southeast, with a popular case of cybercrime known as "Yahoo Yahoo" becoming alarming in the zone (Edeh, 2023). The Economic and Financial Crimes Commission (EFCC) received reports of cases of online scams in the region, with many victims losing millions of naira (Ugwu, 2024). A study by the University of Lagos found that many online stores in Nigeria are fake, with customers

being scammed into buying counterfeit products (University of Lagos, 2018).

- **Data breach**: Cybersecurity breach, according to Juneja, Goswami, and Mondal (2024), can expose personal data, trade secrets, and confidential information, leading to financial and reputational damage. Cybersecurity breaches in South East Nigeria include the 2019 attack on the United Bank for Africa (UBA) and the 2020 hack of Paystack, resulting in the theft of millions of naira from customers' accounts (Techpoint Africa, 2020)
- **Shortage of cybersecurity skills and expertise;** there is a shortage of skilled cybersecurity professionals and inadequate training programs, which hinder organizations from implementing effective strategies and responding to evolving cyber threats.

- **Lack of Awareness and Education; many** individuals and businesses lack awareness of cybersecurity risks and best practices, leading to poor hygiene and increased vulnerability to phishing attacks and malware infections, thereby escalating cybersecurity risks across the region.

The Impacts of Cybersecurity on the Digital Economy

The impacts of cybersecurity on the digital economy in South East Nigeria can be both positive and negative, influencing various aspects of business operations, economic growth, and societal trust.

Positive impacts

- **Protects sensitive information;** the personal data, trade secrets, financial information, and intellectual properties of the firm are highly protected from theft and damage (Kala, 2023)
- **Trust and confidence;** the use of digital services is encouraged by strong and advanced cybersecurity measures, which also promote trust and confidence in the digital economy. According to Juneja, Goswami, and Mondal's (2024) analysis, trust and confidence boost higher and continuous use of digital services, which promotes the digital economy.
- **It promotes the growth of the economy and investment;** a secure digital environment in the region can attract both domestic and foreign investments, as it protects digital assets and intellectual property from cyber threats. This environment also encourages businesses to innovate and expand their digital services.
- **It promotes innovation and the advancement of technology;** the investment in the cybersecurity sector promotes innovation, encouraging the development of new cybersecurity products and services, and strengthening the digital economy.
- **Job creation;** The increasing importance of cybersecurity in the digital economy has boosted the demand for skilled professionals in fields like cybersecurity experts, IT experts, data analysts, among others, thereby creating job opportunities, and contributing to the digital economy growth of the South East region.

Negative impacts

- **Financial loss;** Cyber-attacks involve stealing of personal identification, and carrying out fraudulent activities, leading to significant financial losses to businesses and individuals results in a decline in the digital economy's overall financial health.
- **Loss of consumer confidence;** Cyber-attacks can undermine consumer confidence in online transactions and e-commerce platforms, leading to a decline in the growth of the digital economy. Consumers may become reluctant to conduct online transactions, leading to a significant decrease in the volume of digital commerce.
- **Disruption of business operations**: Cyber-attacks like ransomware, malware, DoS, and data breaches can disrupt business operations, causing loss of productivity and revenue, especially for digital businesses like e-commerce platforms and financial institutions, and damaging customer trust. 60% of small businesses are victims of Cyber attacks and are permanently shut down within six months (Business Day, 2022).
- **Damage to reputation and brand equity**: Cybersecurity breaches can damage an organization or firm's reputation, brand equity, and customer perception, leading to negative publicity, media scrutiny, and long-term market competitiveness in the digital economy.
- **Stifled innovation and digital transformation;** Cybersecurity fears can hinder businesses from adopting digital innovation and adopting transformative technologies, potentially reducing investments and stifling growth opportunities in the digital economy.

CONCLUSIONS

The digital economy relies entirely on cyberspace. The overall health of the digital economy lies in cybersecurity; cybersecurity is the cornerstone of the digital economy. A cybersecurity attack can lead to less or no growth and advancement of the digital economy. It is pertinent to understand the threats and challenges of cybersecurity on the digital economy. These threats include cyber attacks (malware, phishing, ransomware, etc.), cybercrime, and a lack of advanced cybersecurity infrastructure, among others. Cybersecurity incidents can have both positive and negative impacts on individuals, institutions, organizations, and the government, causing direct financial loss and reputational damage.

We provided an overview of the digital economy, explaining how cybersecurity impacts its growth. We argued about the state of the digital economy in the South East region of Nigeria using the pillars of the digital economy as a yardstick of evaluation. We also looked into the threats and challenges posed by cybersecurity on the digital economy, looking at the negative and positive impacts on the digital economy of the South East, and concluded that there is a need to provide advanced cybersecurity infrastructure to tackle threats, and collaboration among the public and private sectors, among others.

RECOMMENDATIONS

- There should be investment in the development of digital infrastructures in the region, such as a digital forensic lab, fiber-optic cables, and mobile internet access, and reduce cyber threats
- Regularly educate employees, businesses, and the public on cybersecurity, including phishing prevention, strong password usage, and data security through workshops, seminars, and awareness campaigns.
- To protect digital assets and sensitive information, deploy robust cybersecurity measures like firewalls, antivirus software, IDS, encryption, and multi-factor authentication for enhanced access controls.
- There should be potential mitigation, such as prompt patching, avoiding unauthorized software, and rolling out stronger monitoring practices through a detection system.
- Conduct regular cybersecurity assessments and audits to identify vulnerabilities and assess security controls.
- Promoting collaboration among businesses, government agencies, and cybersecurity professionals through forums, information-sharing platforms, and industry alliances, fostering the exchange of threat intelligence and best practices.
- allocating resources for cybersecurity infrastructure upgrades and supporting, investing in advanced technologies, threat intelligence platforms, and data analytics tools.

REFERENCES

Cybersecurity Ventures. (2020). Cybercrime damages $6 trillion by 2021. Retrieved from https://www.cybersecurityventures.com. Accessed on July 30th, 2024

Ekpeke, M (2024, March 26). Expert highlights key challenges of Nigeria's pursuit of a digital economy. ITPulse. www.itpulse.com. Accessed on July 30th, 2024

Freijat, S.Y (2023). Digital economy: its characteristics, advantages, applications. www.researchgate.net Accessed on July 30th, 2024

Hardin, R. (1968). The Tragedy of the Commons. *Science, 162*(3859), 1243–1248.

IMD. (2023). IMD World Digital Competitiveness Ranking 2023. Retrieved from https://www.imd.org. Accessed on July 30th, 2024

ISACA (2015): Global Cyber Security Status Report, *ISACA, Rolling Meadows*, Illinois, USA.

Juneja, A, Goswami, S.S., & Mondal, S (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. *Journal of Technology Innovations and Energy* 1-22

Kala, E. (2023). Critical Role of Cyber Security in the Global Economy. *Open Journal of Safety Science and Technology, 13* 231-248

Ladipo, E (2022, January 14). Nigeria businesses suffer 2308 cyber attacks every week. *Business Day*. www.businessday.ng Accessed on July 30th, 2024

Lesmana, D., Afifuddin, M., & Adriyanto, A. (2023). Challenges and Cybersecurity Threats in Digital Economic Transformation. *International Journal of Humanities Education And Social Sciences (IJHESS) 2(6)* 1917 – 1924

Spremić, M, & Šimunic, A (2018). Cyber Security Challenges in Digital Economy; *Proceedings of the World Congress on Engineering*

Boyer, M. A, & Butler, M J. (2006). Public Goods Liberalism: The Problems of Collective Actions," in Jennifer Sterling-Folker (ed.): *Making Sense of International Relations Theory*, Boulder/London: Lynne Rienner, 75–91.

Olson, M (1965). *The Logic of Collective Action: Public Goods and the Theory of Groups,* Cambridge: Harvard University Press.

Mulligan, C., (2017). Cybersecurity: cornerstone of the digital economy, in Imperial College Business School, London, Imperial College London: London.

Musgrave, R. A. (1959). *The Theory of Public Finance: A Study in Public Economy*. McGraw-Hill.

Nguyen, O (2023). Digital Economy and Its Components: A Brief Overview and Recommendations. MPRA Paper No. 116110, https://mpra.ub.uni-muenchen.de/116110 Accessed 16th July 2024

Nsekpong, U. (2022, May 10). Top hubs in South East Nigeria, history, and innovations that will shock you. Techforest. www.techforestng.com Accessed on July 30th, 2024

Nwankwo, J (2023, November 16). How e-commerce startups blew a two-year-old weekly sit-at-home opportunity in the Southeast of Nigeria. www.techeconomy.ng Accessed on July 30th , 2024

Nwankwo, J (2024, February 5). Zuwanu is bridging markets, empowering Imo state's e-commerce revolution. www.techeconomy.ng Accessed on July 30th, 2024

Olson, M. (1965). The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press.

Osamuyi, O (2016, September 20). MadeInAba.com.ng, an e-commerce platform for products made in Aba, is launching on October 1. www.techcabal.com Accessed on July 30th, 2024

Public Safety Canada. (2014). Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada. http://www.bt-tb.tpsgc-pwgsc.gc.ca/publications/documents/urgence-emerge Accessed on July 30th 2024

Samuelson, P. A. (1954). The Pure Theory of Public Expenditure. *Review of Economics and Statistics, 36(4),* 387-389.

Florini, A. (2003). *The Coming Democracy: New Rules for Running a New World*. Brookings Institution Press.

Teoh, C.S & Mahmood, A.K (2017). National cyber security strategies for digital economy *Journal of Theoretical and Applied Information Technology 95(23)* 6510-6522

Ukwuoma, H, C., Williams, I.F & Choji, I.D (2022).Digital Economy and Cybersecurity in Nigeria: *Policy Implications For Development. International Journal of Innovation in the Digital Economy 13(1)* 1-15

Ugwu, C (2024, May 8). Court jails 41 internet fraudsters. *Premium Times*. www.premiumtimesng.com Accessed on July 30th, 2024

Umeh J (2022, March 2). Internet penetration: why Southeast remains the lowest at 13.7million users. *Vanguard.*www.vanguardngr.com. Accessed 17th July 2024

Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into a business transformation*. Cambridge: Harvard Business Press.

Izuaka, M (2023, August 23). Nigeria ranked 11th in global internet penetration, NCC. *Premium Times.* www.premiumtimesng.com Accessed 18th July 2024