


Digital Economy and Cybersecurity in Nigeria: Policy Implications For Development

Henry Chima Ukwuoma, National Institute for Policy and Strategic Studies, Kuru, Nigeria*

 <https://orcid.org/0000-0002-2819-7146>

Ifeanyi Solomon Williams, National Institute for Policy and Strategic Studies, Kuru, Nigeria

Ibrahim Dinju Choji, National Institute for Policy and Strategic Studies, Kuru, Nigeria

ABSTRACT

The COVID-19 pandemic has resulted in the urgent need for the Nigerian government to embrace digital economy at all costs. Countries with digitised economies have been able to easily adapt to the challenges that the pandemic has brought, such as eLearning for the education sector and e-business for the business sector. This innovation, however, comes along with a lot of cyber-attacks by cybercriminals resulting for the need to establish adequate cybersecurity measures. Nigeria has gravely felt the impact of the COVID-19. Businesses have been shut. Countries have shut their borders, thus making it impossible for Nigerian government/businesses to access other countries' products, most especially China. The paper reviews the digital economy of some developed nations and their cybersecurity measures to sustain this innovation. The study further highlights how Digital Economy has contributed to the Gross Domestic Product of most nations, thus serving as a means of diversification for most nations.

KEYWORDS

Cybercrime, Cybersecurity, Cyberspace, Digital Economy, Internet, World Wide Web

1. INTRODUCTION

The invention of the World Wide Web in 1989, led to the innovation of the first-ever website on the internet in 1991. This development led to the establishment of over 1.5 billion websites with Governments, private organisations, individuals and businesses exploring the potentials of the cyberspace (Internet Live Stats, 2020). The existence of websites has constituted a major requirement for most institutions in the global environment, hence making the world a global village. This invention has generated other innovations that are being driven by the internet/cyberspace. Government, Private and public enterprises now carry businesses in the cyberspace for the sake of ease, convenience and accountability. This has led to criminals on the internet who are referred to as cybercriminals deploying all sophisticated means to defraud vulnerable persons, business and governments. Interestingly, there are 3.8 billion Internet users, which accounts for fifty-one (51) percent of the world's total population of 7 billion (ITU, 2020).

The dependency by Institutions/Governments and Businesses on the cyberspace implies that there is urgent need for an enhanced cyber security to guarantee a governed cyberspace.

DOI: 10.4018/IJIDE.292489

*Corresponding Author

COVID 19 has necessitated the transactions of most businesses, communications, interactions, to occur in the cyber space, thus constituting the dependence and survival of governance, businesses and communication on the cyber space. Additionally, most persons rely on visual means of communication, Meetings, Conferences with Apps such as Zoom, Skype, etc, but the question remains who monitors/regulates these applications and how secured are they. The dependence of office work and communication via the cyberspace because of the Coronavirus has resulted to an increase in cybercrime and has provided an environment where scammers and hackers thrive. Common cybercrimes during this pandemic include: phishing and ransomware while social engineering is also on the rise (FBI, 2020). Social Engineering is described as the art of manipulating people to give up their confidential information. This art is on the rise amid the coronavirus pandemic.

Most digitalised economies have been targets of these cyberattacks. Countries such as the USA, Singapore, China, Germany, United Kingdom, Russia, has recorded most cyberattacks even before the COVID-19 pandemic, now records much more cyberattacks on daily basis. The countries that have embraced digitalisation, have excelled in areas such as the digital innovation, digital industry, digital facilities and digital governance.

Severally, the governments of USA and UK have been victims of data hijacking because of its digital economy, and the USA has come out to state that its coronavirus data is on the threat of being hijacked by cybercriminals from other nations (Chohan, 2020). For developed countries whose economy is digitalised, a hijack or manipulation of COVID 19 data will imply slowing down the response to the crisis. For example, robots and drones are being used by the US, China, South Korea and other countries, if hijacked could affect the management of the pandemic crisis situation. Such attacks pose danger to the health and safety of patients during a COVID 19 pandemic that is over stretching most country's health care systems. This has necessitated an increased cybersecurity in mostly the health and financial sector of the digitalised economies of most nations.

It is pertinent to note that a guaranteed cybersecurity by governments implies an enhanced human security. Human security is described as an approach in identifying and addressing widespread and cross-cutting challenges to the livelihood, survival and dignity of people, which calls for people-centred, comprehensive, context-specific and prevention-oriented responses that strengthen the protection and empowerment of all people (United Nations, 2020). It is argued that security should be seen at the human/individual level rather than at the national level. Which raises the question, does cybersecurity enhance promote human security? The Nigerian government has commenced the digitisation of her economy and this raises the issue of its readiness to provide an efficient and effective cybersecurity. Digitisation denotes services of a country are all going online which implies that there is need for an efficient and effective cybersecurity measures in the Nigeria cyberspace. Digital economy is perceived as internet economy where businesses are performed on the cyberspace. Unfortunately, famous digital economies in the world such as the USA, China and Russia are being faced with series of attacks on a continuous basis, which also raises the question of how safe these economies are and how prone they are to cyber-attacks.

According to the Global Security Index Report (2018), cyberattacks across the world have centred on five industries which include, Government, financial services, transportation, manufacturing and health care; predicting that cybercrime will cost worldwide damages, which may account for about \$6 trillion annually by 2021, up from \$3 trillion in 2015 (Cybersecurity Ventures, 2020). The question remains, who will take the lead for the fight against cybercrime, what measures have been put in place by governments to protect the vulnerable against such cyber-attacks. The cyber space systems are designed in such a way that most times a human intervention is needed before monies can be pushed out of one's bank account, yet people fall prey to the devilish acts of these cybercriminals. Conversely, cybercriminals use all kinds of sophisticated tools and means to perpetuate their crimes and hence making it very difficult to trace them and are increasing in numbers on a daily basis. (CNBC, 2017)

With the coronavirus pandemic ravaging its way into the society and forcing governments, organisations, businesses and persons to work and stay at home, these cybercriminals have taken the

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/digital-economy-and-cybersecurity-in-nigeria/292489

Related Content

Evolution, Development and Growth of Electronic Money

A. Seetharaman and John Rudolph Raj (2009). *International Journal of E-Adoption* (pp. 76-94).

www.irma-international.org/article/evolution-development-growth-electronic-money/1832

Student Technology Projects in a Remote First Nations Village

Tish Scott (2007). *Information Technology and Indigenous People* (pp. 137-140).

www.irma-international.org/chapter/student-technology-projects-remote-first/23546

Measuring the Acceptance of Internet Technology by Consumers

Donald L. Amoroso and Scott Hunsinger (2009). *International Journal of E-Adoption* (pp. 48-81).

www.irma-international.org/article/measuring-acceptance-internet-technology-consumers/37578

Routing Protocols Design and Performance Evaluation in Wireless Mesh Networks

Mohsen S. Alsaadi and Naif D. Alotaibi (2019). *International Journal of Technology Diffusion* (pp. 60-74).

www.irma-international.org/article/routing-protocols-design-performance-evaluation/219334

Indigenous Knowledge Intelligence and African Development

Alexander Maune (2017). *Handbook of Research on Theoretical Perspectives on Indigenous Knowledge Systems in Developing Countries* (pp. 173-197).

www.irma-international.org/chapter/indigenous-knowledge-intelligence-and-african-development/165744