**International Journal of Cyber Research and Education**
Volume 3 • Issue 1 • January-June 2021

# Cybercrime:
## An Emerging Threat to Economic Development in Nigeria

Henry Chima Ukwuoma, National Institute for Policy and Strategic Studies, Kuru, Nigeria
https://orcid.org/0000-0002-2819-7146

## ABSTRACT

This paper presents the nature, effects, and dynamics of cybercrime in Nigeria and its effects to economic development in the country. The paper is sourced for secondary data through, journals, periodicals and publications as well as obtained primary data from the field. Primary data was sourced through the distribution of 66 questionnaires using the purposive sampling technique. Findings revealed that there exists an insecure cyberspace in Nigeria and the activities of the cybercriminals affects the economy negatively by discouraging Nigerians from partaking in electronic services/transactions, thus discouraging Nigerians from accepting the concept of digital economy. Findings also revealed that activities such as unauthorized access, hacking and cracking, online fraud, identity theft, cyber terrorism, amongst others were dominant threats in the cyberspace and finally the cyberspace provide jobs and by implication contribute to the socioeconomic development of the Nigerian State. Recommendations proffered include the federal government to train and retrain forensic experts in all financial/security agencies towards achieving a secured cyber space and the need for the federal, state, and local governments to create awareness amongst others.

## KEYWORDS

Cybercrime, Cybersecurity, Economy, ICT

## INTRODUCTION

The advent of the internet has revolutionised the present society by driving and sustaining economic growth in developed and developing countries hence providing a platform for a new means of communication and making the world a global village. Cyberspace has opened up societies and cities to the technology driven world and also to threats. Most digital information and transactions are carried out stored in the cyberspace and are susceptible to attacks.

Nigeria has a population of over 200milliom (World Bank, 2019), with a staggering 258,493,026 Mobile GSM users, as of November, 2018. In 2019, the Nigerian Communication Commission revealed that about 160 million people subscribed to the internet (NCC, 2019; Punch, 2019a) though Nigeria is rated 47 in the world as it relates to the number of internet subscribers. The ITU Connect 2030, suggests that there will be 70 per cent Internet penetration by 2023 worldwide, thus the need a for a secured cyber space (GCI, 2018).

DOI: 10.4018/IJCRE.2021010102

The number of GSM users and internet subscribers increases on a monthly basis; the question remains; are these subscribers secured in the Cyberspace. Most activities are presently carried out via internet and being relied upon to serve as medium to service-oriented operations but it should be noted that the over reliance on the cyberspace exposes persons/businesses to cyber-attacks/threats.

Cyberspace is an international and unstable domain which is identified by the use of electrons and electromagnetic spectrum whose aim is to create, modify, store, exchange, extract, use and delete information without a sole administrator (Mayer, 2014). Nigeria being on the international domain benefits from the existence of cyberspace. As a developing country with a growing economy, Nigeria stands a greater chance of benefiting from this space because of her population which is fast growing and also serves as a market hub for Africa (Ukwuoma, 2019). Such benefits include; serving as an information resource, serves a medium of communication, and social networking (Majid, 2012).

The cyberspace has assisted developing/developed countries grow and sustain its economy. These benefits come with a major challenge, which is cyberattacks. Countries such as the USA, UK and Russia with the best and stringent cyberspace security measures have suffered setback, as attacks and fraudulent activities has affected citizens, businesses and Government and has made the cyberspace community to operate with caution (Oulsola, et al., 2014). These fraudulent activities are carried out with the sole aim of financial gains by attacking bank accounts of individuals, businesses and governments. Information Technology (IT) contributes immensely to the Nigerian economy and other developed countries such as the United States and United Kingdom, however IT exposes citizens, firms and States to the danger that are often been perpetuated in the Cyberspace.

The number of cyber criminals in Nigeria and around the world is on the rise because interconnectivity and communication medium via the cyberspace has also increased, which has made it extremely difficult to apprehend and persecute these cyber criminals with their targets been any IT or IT related devices/services. The persistence of cybercrime is in on the rise because it is easy to execute and very rewarding, the FBI in collaboration with the EFCC, currently released/published a list of Nigerians who are on the most wanted list and defrauded individuals and companies of like sum, although, this has sounded a warning to those who intend to and currently practicing the act to desist or face the wrath of the law.

According to a report of the Council of Economic Advisers to the President of the United State (2018), a cyber activity could be regarded as malicious activity if an unauthorized user tries to mar the privacy of available information/communication systems or could be referred to as an activity to attack the confidentiality, Integrity and Availability (CIA) of information or computers (Naser and Zolkipli, 2013). It is based on these activities that countries have developed cybersecurity measures to curb the activities of unauthorized use. The Federal Bureau of Investigation alongside other investigative bodies have tried to clamp down the activities of cybercriminals through collaboration with States yet the crime activities still persist. In 2017, the Director of National Intelligence in the United States posited that the activities of mischievous elements in the cyberspace is on the increase and has degenerated to become the strategic threat to the government and industry sources, malicious cyber activity is a growing concern for both the public and private sectors and further stated that cyber threats were the most important strategic threat challenging the US economy and the world economies at large.

Mbanaso, Chukwudebe and Atimati (2015) posits that socio-economic, political and cultural activities of every State is currently driven by cyberspace and could cause serious damage if it interrupted or collapses. They also suggested that the internet which is also referred to as the cyberspace has become a platform for war, novelties, networking and criminality.

The Nigerian Communication Commission (NCC) is saddled with the responsibility to regulate the cyberspace and the commissions' effectiveness led to the internet availability to rural and urban areas in the country. It all started with the use of VSAT technology and then the GSM, 3G, 4G and presently the provision of testing ground of the 5G technology (NCC, 2019). Interestingly, these trends provided jobs for the unemployed youths and provided a platform for business to thrive in