INTERNATIONAL JOURNAL ON ECONOMICS, FINANCE AND SUSTAINABLE DEVELOPMENT

IJEFSD

Available online at www.researchparks.org

RESEARCH PARK

Journal homepage: www.researchparks.org/

Cybercrimes and Economic Crisis in Nigeria: Essentialising Containment Beyond the Rhetoric

Emmanuel U. Awak, PhD

Department Of General Studies, Akwa Ibom State Polytechnic, Ikot Osurua, Nigeria

constructcritics@yahoo.com

ABSTRACT

Just as the emergence of Internet and ICT innovates, instigates and transforms all facets of life and sectors of the society; so also, is the tenacity, tempo and geometric penetration of cybercrimes. The devastating consequences including economic doldrum, low gross domestic product (GDP), inclement investment environment, loss of billions and confidence through e-fraud, e-scams, data interception, and system and data interference, among others beckon decisive inhibition. However, slow and ill-implementation of legislation, lack of virtual evidence, knowledge of investigation and parochialism has continued to define most actions to protect the cyberspace. The paper qualitatively through social survey and multi-stage sampling methods examines parameters of cybercrimes as one of the enablers of economic crisis in Nigeria, using Akwa Ibom State as a specific study site. The discourse is shaped within theoretical frame of Situational Crime Prevention (SCP), since its strands are descriptive of the ravaging circumstances of cybercrimes, cybercriminals, and the obtuse and ductile tactics toward containment of cybercrimes. The result indicates that cybercrimes have strangulated the economy, and that its prevalence and spate annihilate germane quest for economic recovery. Therefore, utilisation of data surveillance technologies, SCP intervention techniques, cybercrimes' awareness and education, intelligence-policing, faithful legislation and implementation are recommended.

ARTICLEINFO

Article history:

Received 20 Apr 2022

Received in revised form 20 May 2022

Accepted 25 Jun 2022

Keywords:

Cybercrimes, containment, CRAVED, economic crisis, SCP intervention techniques.

E-mail address: info@researchparks.org

Peer review under responsibility of Emil Kaburuan.

Background

Cybercrimes are any illegal acts committed within a computer network or facilitated by the use of a computer or electronic system, (Comer, 2006). They are committed by hacking (getting unauthorised access to a computer system) and it comes in many forms ranging from password sniffing, web cramming, spoofing, credit card fraud, identity theft, data kidnapping through industrial espionage, software piracy, to cyber fraud that involves stocks manipulation or fraudulent business deals, as well as computer sabotage and cyber terrorism, (Awak, 2019a). Infact, Wall (2001) posits that cybercrime is as sophisticated as the modern technology, and it has the capacity to massively destroy or disrupt the social, economic, political order and stability.

The most worrisome is that the pervasiveness of these emerging crimes seems not to be appreciated in Nigeria despite the debilitating effects, just as the presence of Economic and Financial Crimes Commission (EFCC), who sometimes, plays to the gallery through media trial but fails to cover much of the grounds of cybercrimes have not remedied the situation, (Awak, 2019a). This explains why the Nigeria Army in 2020 left its constitutional duties to join in countering cybercrimes before the #EndSARS protestations disrupted the operation.

Many countries, including the United States understood that the economy, in the voice of Karl Marx, is the infrastructure upon which other institutions are rested. This assertion, perhaps, might have informed their swift action to criminalise hi-tech-crimes of any magnitude. These include making, possession or distribution of certain material, such as child pornography, fraud, among others, (Joseph, 2003; Yar, 2006). However, in Nigeria, it took the federal government over fifteen (15) years to enact a law on cybercrimes (Protection, Prevention, etc.) Act (2015) after it set up the Nigeria Cyber Working Group (NCWG) in 2000.

That Nigeria is forced to romance with information and communications technologies ICTs) is a bitter pill that must be swallowed as inadequate safety measures to monitor and police the system and its processes (in spite of the existence of an International Convention on cybercrime) suggest. But this does not negate the exponential rate at which ICTs and their applications have spread. Financial, psychological, political and economic losses recorded through cybercrimes are underpinnings of the amazing capabilities of the youths to manipulate related devices that sometimes, are deleterious to Nigeria's economy and overall well-being. That the economy is stultified by activities of cybercriminals in addition to Covid-19 pandemic debacle is worrisome, making containment strategies imperatives.

The above background is the foundation upon which this paper and its essence are rested, with a view to bringing the challenges of cybercrime to the public domain with necessary suggestions.

Study Objective

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

The core objective of the paper was to empirically collect data and as well, analyse containment measures as advocated by SCP in order to gauge how effective they have been in curbing or ameliorating the strangulating pangs of cybercrimes.

Pertinent questions

a. How can cybercrimes containment move beyond the usual patterns of discourse (rhetoric)?

b. What are the perceptions of the people toward cybercrimes and various strategies adopted to curb the menace?

c. To what extent have cybercrimes affected negatively the financial and economic activities in Nigeria?

Conceptualisations

Cybercrimes: This refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. Additionally, although the terms **computer crime** and **cybercrime** are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, (Awak, 2019a; Wall, 2006). These terms are also used to include traditional or conventional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. As the use of computers has grown, computer crime has become more important, (Furnell, 2002).

Gantz and Rochester (2005) and Wall (2001) conceive of computer crimes are actions or inactions wittingly targeted at information technology infrastructure, including illegal access interception, data and systems interference, misuse of devices, forgery and electronic fraud.

According to Awak (2019a), the pervasiveness of cybercrimes involving hacking, copyright infringement, pornography, fraud and racketeering of varied dimensions has created a subculture of organised crimes and criminals. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Computer crime encompasses a broad range of potentially illegal activities, (Turkle, 1995).

Containment: This has to do with activities including regulation and control, prevention, more remedial courses of action that are designed to curtail the commission of cybercrimes. These actions or strategies are mostly proactive in nature, which are tagged along the concept of problem-solving policing.

Cybercrime Legislation: Cybercrime legislation is the process of formulating laws that guide the operations and activities of people in relation to Internet. It is a dynamic body of rules and its apparatuses (cyber-police and cyber-lawyers) (Peng, 2005).

Social Engineering: As used in the study, this is a term that denotes the practice of tricking or deceiving people into giving out or revealing confidential or personal information such as passwords, PIN, BVN, Card number, among others. It involves the exploitation of weaknesses in people, their ignorance and vulnerability, rather than obtaining such information through manipulation of any software.

Economic crisis: It is a period that families are hit hard since breadwinners no longer work; government is grappling with provision of essential services, while the country's currency may devalue thereby, leading to too much money purchasing too few goods. It is a period of great uncertainty, where investors and consumers are petrified by economic outlook. It is empowered by recession, economic downturn or meltdown and divestments, collapse of critical infrastructure, and odious activities of old

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

and emerging cyber manipulators, leading to loss of billions that strangulates the already worsened condition of the people.

The above backdrop typifies Nigeria's economy in recent times. An economy that is beclouded by double digit inflation rate, high unemployment rate, insecurity, health and psychological challenges. It is one with over 70% rate of poverty, high budget deficit and unceasing penchant for borrowing. Indeed, any country romanticising these economic indices is one whose economy is in crisis.

Cyber Criminals: Cyber criminals constitute children and adolescent, organised hackers, professional hackers/crackers and disgruntled or corrupt members of staff or former employees**.**

Literature

Although, a society in the conception of Emile Durkheim that does not experience crime is not a normal one, but when the speed, spate and frequency at which crimes are committed become ingrained in the socio-political and economic life of a nation, the case is unfathomable and alarming. This is why Awe (2006) opines that embezzlement of official funds; trafficking of persons and drugs over the net; the emergence of mafia boys and yahoo-yahoo boys are debilitating to the national economy. As observed by Akosile (2005), sophisticated letters, proposals and business ideas are developed with a view to defrauding unsuspecting investors and they are damaging to the economy, while leaving the image of the country seriously battered. With the rise of social media platforms, the rate at which marriages are broken as a result of new found "love on the net" is frightening and quivering, even the moral fabrics and conscience collective of families and societies are not spared, (Awak, 2019a). Again, the phishing and vishing are contingent to privacy abuse, and has raised global concern on cyber-espionage. Indeed, the September 11, 2001 attack at World trade centre, the Pentagon, Boko haram and bandit invasions, kidnapping and other terrorist attacks are perfected and sustained through the net, and have devastated global security and economic concerns, (Awak, 2019a).

Forensic specialists tasked with investigating computer-related crimes also face new tasks arising from the use of encryption and access protection which has posed a growing challenge of extracting evidence from computers and servers, (Chan, 2001). The implications of such activity for infrastructure protection are ominous, (Semple, 2004). The online availability of source code and automated 'easy to use' hacking tools is a problem (Smith & Rupp, 2002). For instance, they act as system reconnaissance that provide multiple exploit tools by deploying 'spy-ware', (Koziol, 2003). This has increased the risks of computer intrusion activity that could serve as a predicate to other criminal activity such as extortion, financial or Internet fraud, identity theft, telecommunications theft, and economic espionage, (Broadhurst, 2003).

The Internet has created a cybercrime-fraud platform where multifarious types of fraud are committed over computer networks, making effective policing almost impossible. In computer chat-rooms, message boards, unsolicited e-mail, and on web sites, fraudsters lose no opportunity to trick and deceive others for the purpose of financial gain, (Goodin, 2008). Those who engage in fraud operate globally on 'Internet time', 24 hours a day, 7 days a week. Although, many of the schemes perpetrated online in recent times are nothing more than repackaged versions of their 'real world' counterparts, (Grabosky, 2001); however, the efficiency and speed of the network create new opportunities for criminals, while simultaneously positing serious criminal threats to e-commerce, e-government, e-education, e-legislation, e-policing, among others, (Goodman, 2001).

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

In Nigeria, the introduction of Automated Teller Machines (ATM), cashless policy, e-banking and the rate of unauthorised withdrawals; revelation of bank details of victims' accounts and cloning of ATM and other identity cards are just few of the harms experienced; while sales of examination scripts over the net, E-mail scam and copyright infringement through warez, child pornography and child grooming, malware and malicious code, denial of service attacks, viruses, cyber stalking and information warfare are damaging to the computer system, Internet services, private individuals, groups, as well as governments. The geometrical effects of these crimes in the face of ignorant or ill-equipped security agents and normlessness leave much to be desired, and are purveyors of glowing cybercrimes in Nigeria as they avail much unfettered opportunities to suspected cybercriminals.

According to Awak (2019a), News Agency of Nigeria in February, 2008 had cause to review its news dissemination procedure in response to embarrassing and false information that purportedly emanated from it and which subsequently led to the closure of Channels TV by the presidency. Also, Thisday Newspaper had to swiftly react to some misleading /fake information on its digital edition by issuing a notice of disclaimer to its online readers following the invasion of its server by hackers that posted unauthorised/ fake editorial materials in its August 27, 2021 edition (https://punchng.com/thisday-disowns-fake-publication-on-uzodinma-seeks-culprits-arrest/). Hackers also invaded computer systems of a leading Telecom Service Provider in Nigeria and defrauded the company of its airtime worth about ₦10.5million naira (Guardian, October 7, 2008 in Awak, 2019a).

At global scale, cyber criminals are not resting as they attack virtually everything and organisation of interest to them. For instance, in February 2000, Yahoo! website was attacked for three hours (Burke, 2000). On 3rd August, 2000, Canadian federal prosecutors charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks on Amazon.com, eBay, Dell Computer, Outlaw.net, and Yahoo. MafiaBoy had also attacked other websites (Krebs, 2006). Hacking or gaining unauthorised access to a computer system, programmes or data, opens a broad field for inflicting damage (Rehmeyer, 2007). While people who had sent nude images to friends or stored in the net for their privacy, but their systems or social media page like Facebook, Instagram or WhatsApp was hacked have been blackmailed into helplessness, (Awak, 2019a).

With ineffective, inoperable and lopsided implementation of the extant laws, high rate of illiteracy, joblessness and ritualisation of the social media, cybercrimes in Nigeria have become subversive. The suspected criminals are undeterred by the prospect of arrest or prosecution or the presence of the leeway to plea-bargain or the leniency of the punitive measures. The situation is aggravated by e-governance, where government has moved from analogue bureaucracy to digital without compensatory preparation and alertness. Indeed, cyber criminals around the world lurk on the 'net' as an omnipresent menace to the financial and economic health of businesses and the society. Appreciating the magnitude of this problem, as well as devising possible containment strategies underscores the essence for theorisation.

Theoretical Stance: Situational Crime Prevention Theory (SCP), Roland Clarke (1995)

Proponents of SCP are not comfortable with over-reliance on the use of formal punishment to serve as a deterrent, instead, they have advocated for situational interventions before crime of any dimension occurs. They claim that laws and punishment are too distant a threat to influence most offenders' decision-making during crime event, (Braga & Kennedy, 2012; Felson, 2008). Some of the interventions (such as raising high fence with burglary proof makes it difficult for offenders to scale it to gain entry) make it more difficult for the crime to be committed. These interventions assume that persons will choose to conform because the increased costs no longer make it "worthwhile" to commit the crime.

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

SCP recognises that interventions and offender's decisions must converge. Interventions that are temporally distant from crime scenes are usually ineffective. SCP, like general deterrence theory, assumes there is a role for publicity in reducing crime. Bowers and Johnson (2005) explain that publicising SCP interventions will educate the public to take actions that raise the costs of offending to a potential perpetrator by increasing their risk of apprehension. Also, publicity can be used to influence offenders' perceptions of the difficulty, as well as risks of committing a crime and their likelihood of being caught.

SCP is imbued with the question of how offenders successfully commit their crimes. It is the process of appreciating how the offender carries out crime that forms the basis or design interventions that would remove crime opportunities and thereby, preventing offending. This method is obverse to dispositional bias, (Clarke, 2009). SCP basically seeks to solve and reduce crime problems in an action setting. Indeed, SCP's focus on crime reduction has led to partnerships between academics, police, and practitioners, where SCP principles have been used to guide practice, (Braga & Kennedy, 2012; Scott & Goldstein, 2012). To Eck and Madensen (2012), SCP is associated with problem-oriented policing, which the most is leading policing strategy.

Problem-oriented policing gears towards focusing on specific problems to devise proactive strategies to eliminate them, (Clarke & Goldstein, 2003). This, of course, is different from the security operatives' conjectures in Nigeria, where "they are always on top of the situation" and the offenders will euphemistically "pass through under the situation".

Point of intervention

Clarke (1999) identifies characteristics of situations that attract offenders or facilitate their behaviours. This resulted in the idea of "hot products," which led inevitably to the examination of ways in which products could be designed so as to make them less desirable to thieves, (Ekblom, 2012a). This means that the point of intervention is not at the site where the crime might occur, but at the earliest possible point, the design of the product and service that might be stolen. The characteristics of "hot products and spots" are associated with the acronym **CRAVED**, (Clarke, 1999):

- **Concealability:** Any objects or items that can be hidden in pockets or bags are more easily stolen by shoplifters and other sharp thieves.
- **Removability:** The fact that cars and bikes are mobile helps explain why they are so often stolen. It is equally justifiable by its nature that laptops, phones and other ICT related devices are portable and susceptible to being stolen with ease.
- **Availability:** The rising wave of cybercrimes is as a result of the availability of attractive new products, such an iPhone, Notebook, callcards and other gadgets, and the illegal markets for selling such products. Desirable objects that are widely available and the ease to find are at higher risk.
- **Valuable:** Criminals will generally choose more expensive goods, just as cybercriminals including bank officials will attack accounts with fat amount, especially those that are not active for a while.
- **Enjoyability:** Hot products or services may be enjoyable things to consume, such as liquor, tobacco, and songs or videos, and other virtual products, and will be susceptible to attack.
- **Disposability:** Criminals have a preference for products that are easy to sell or dubious ideas that are easily bought by unsuspecting members of the public.

The idea of hot products has led to the insight that crime prevention can be built into the design of products and services in the same way that safety is designed into automobiles, (Ekblom, 2012b; Clarke

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

& Newman, 2005a, 2005b).

Though, SCP's designation is to create interventions that ***eliminate*** all opportunity to commit crime. The reality is opposite because it seems impossible, and SCP's is equally moving towards reduction of the ***amount*** of specific crime and the level of harm caused. For instance, redundant computer systems are designed so that if a hacker destroys one system, the other can replace without any breakdown.

Legislation, Cybercrimes and Threats

Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 enacted by the federal government of Nigeria is specific in **Part 11**, **Subsections 5 to 36** that deal with offences, as well as possible penalties to be paid by offenders when convicted. These include offences against critical national information infrastructure, unlawful access to a computer, registration of cybercafé, system interference, interception of electronic messages, email, electronic money transfers, tampering with critical infrastructure, wilful misdirection of electronic messages, unlawful interceptions, computer related forgery, computer related fraud, theft of electronic devices, unauthorised modification of computer systems, network data and system interference, electronic signature, cyber terrorism, exceptions to financial institutions posting and authorised options, fraudulent issuance of e-instructions, reporting of cyber threats, identity theft and impersonation, child pornography and related offences. Others are cyberstalking, cybersquatting, racist and xenophobic offences, attempt, conspiracy, aiding and abetting, importation and fabrication of e-tools, breach of confidence by service providers, manipulation of ATM/POS Terminals, employees responsibility, phishing, spamming, spreading of computer virus, electronic cards related fraud, dealing in card of another, purchase or sale of card of another, use of fraudulent device or attached e-mails and websites.

For explication, some of these offences are treated here:

Spam: Spam is the sending of unsolicited bulk email to an email account of another person for the commercial purposes, which may include advertisement for new products, admissions, among other products, (Snail, 2009). The negative effect of this act is that when too much are sent, it could lead to the crashing of the account thereby, denying the owner the opportunity to make use of such an account.

Fraud: Computer fraud is any dishonest misrepresentation of fact intended to induce another to do or refrain from doing something which causes loss, (Edelson, 2003). In this context, fraud will result in obtaining a benefit by altering, destroying, suppressing, or stealing output, usually to conceal unauthorised transactions or deleting stored data, and misusing existing system tools or software packages, or writing code for fraudulent purposes, (Gehring, 2004).

Hacking: Hacking means an illegal intrusion into a computer system and/network. It is a process where programmers deploy their expertise into designing various programmes aimed at maliciously bypassing any security gateway to any computer or network of their choice. Hacking is equivalent to cracking, (Hollinger, 1988).

Salami Attacks: These attacks are prevalent in the financial institutions. There is an alteration that is so insignificantly made such that in a single case, it would go normally unnoticed, (Awak, 2019a; Marshall, 1999). A case in point is when a bank employee inserts a 'logic bomb' into the bank's servers, with the aim of deducting a small amount of money (like fifty naira - ₦50.00 a month) from the account of every customer and deposits it in another account opened and owned by the bank staff. Indeed, this could continue for a long time without any obstruction since, no account holder would probably notice this unauthorised debit because it is so insignificant an amount, but it could be very devastating, while the bank employee makes a sizeable amount of money every month.

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

Internet Time Thefts: hese thefts involve the use of Internet surfing hours of the victim by another person. This is done by gaining access to the login ID and the password. Air time could also be stolen from internet service provider or even global mobile system of communication (GSM). For instance, Awak (2019a) reports that MTN of Nigeria sometime in February 2009 suffered serious economic losses when its systems were hacked and airtime of huge amount of naira was stolen. This crime has been a recurring decimal, affecting almost all other service providers.

Research Design/ Methods

To conduct an in-depth study on the subject of investigation, the study resorted to qualitative empirical method using a social survey. This is adopted for various reasons including explanation, description, discoveries or interpretation of some phenomena in the population. Survey research studies involve selecting and studying samples chosen from the populations to discover the relative incidence, distribution, and interrelations of sociological variables. It permits a researcher to study more variables at one time than is typically possible in other methods, (Ukoka & Awak, 2015).

The main techniques of data collection were triangulation, in addition to document analysis. The study adopted Multi-Stage Sampling method. This method facilitated the distribution of the population into various stages of sampling units based on geographic locations. On this basis, Akwa Ibom State was divided into three Senatorial Districts of Uyo, Eket and Ikot Ekpene. The districts were represented by Uyo metropolis, Ikot Ekpene and Eket urban.

The sampling size was four hundred respondents. This consisted of one hundred (100) respondents taken from Eket and Ikot Ekpene urban respectively, while two hundred (200) respondents were selected from Uyo. This was based on the fact that Uyo metropolis is more populated by literate class than any other research sites. With this, respondents were given copies of the questionnaire to supply their responses. The frequency distribution of respondents from this process formed the basis of data analysis.

Findings

Cybercrimes are in existence because computer and other internet architecture are vulnerable sequel to the existence of:

(i) **Complex technology, lapses and negligence:** Cyber criminals rely upon and take advantage of lacunas and negligence to penetrate into the computer system. This could be done by secretly implanting logic bomb (key loggers that can steal access codes), advanced voice recorders; retina imagers, among others. These devices can be utilised to deceive biometric systems and bypass firewalls thereby, deactivating any security system that would have denied any intruder an access to the system.

(ii) **Anomic situation:** Anomie is conceived as a condition in which society provides little moral guidance to individuals, (Gerber & Macionis, 2010). It has to do with a situation where there is breakdown of social bonds between an individual and the community as depicted by the presence of boisterous circumstances emanating from fragmentation of social identity and rejection of self-regulatory values. Accordingly, Durkheim (cited in Ukoka & Awak, 2016) observed that anomie arises more generally from a mismatch between personal or group standards and wider social standards, or from the lack of a social ethic, which produces moral deregulation and an absence of legitimate aspirations. The existence of legislation, but without adequate application is a source of encouragement, instead of deterrence to the commission of cybercrimes. For instance, the non-domestication of the Cybercrimes Act of 2015 by federating states of Nigeria, coupled with free-

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

rein leadership style in application of the letters of the Act to tame the tide of cybercrimes depicts an anomic situation.

(iii) **Prevalence of social vices:** Social vices are acts or behaviours that are negation of the socially approved ways of life in the society. They are activities that people get involved wittingly or unwittingly, which consequences are borne by the actors, family and the society (Awak, 2019b). These acts are not in tandem with the expectations of the society and are injurious to victims. Such acts are regarded as anti-social, anti-people and dysfunctional to the progress and development of the society. A society where there is a prevalence of social vices**,** occasioned by high rate of unemployment and loose moral and social fabric; where the "get-rich-fast syndrome" defines the exploration and exploitation of cyberspace is nothing, but one imbued in social derision. The prevalence of social vices in the society provides sufficient justifications such that getting involved in cybercrimes or acquiring the label of Internet fraudsters called "yahoo-yahoo" in Nigeria is not a big deal. Indeed, the amount of fast and unhindered quantum of money derived from engagement in cybercrimes serves as conduit for perpetuation and enlistment of others into heinous cybercrimes.

(iv) **Opportunities and absence of capable guardians:** Awak (2019a) while discussing theoretical disposition of RAT found that where there is unfettered access to attractive target in the absence of a capable guardian that crime, irrespective of nature and magnitude will occur. Therefore, cybercrimes are commissioned because there are opportunities created by ignorance or carefree lifestyle and the inability of the agents of criminal justice to take conscionable actions aimed at preventing or creating conducive atmosphere for cybercrimes to occur.

(v) **Dimensions and magnitude of electronic fraud:** There are three dimensions to electronic fraud in Nigeria. These include, internal fraud (banking staff); external fraud (ordinary Nigerians), and collaboration between fraudsters and banking staff. Systems and database administrators who have unfettered access to information technology (IT) systems, and related infrastructure of the bank perpetuate this crime.

Between July and September, 2019, Nigerian banks lost ₦552million to fraud related transactions, but as a result of the Covid-19 pandemic and subsequent lockdown in 2020, the loss astronomically peaked at ₦3.5billion within the same period. In terms of medium of commission of fraud, it is noted by Nigeria Inter-Bank Settlement System (NIBSS) that the highest number of fraudulent transactions are committed on the web channels, while financial fraud transacted through phones recorded a loss of ₦410 million that constituted about 11.7 percent of the entire loss value. In 2020, an increasing number of small-medium banks and financial institutions across Africa, Asia, and Eastern Europe were prey to ransomware attacks from groups with expertise in vending remote desktop protocol/ virtual network computing (RDP/VNC) network access. The opportunity existing as a result of modesty of small banks' cybersecurity architecture makes them preferred targets for hacking. With an alarming rise in vicious cyberattacks on financial institutions in 2020, it is now estimated that 10 percent of all data breaches were related to the financial industry. The most prevalent technique adopted in the commission of bank fraud as contained in NIBSS industry fraud report is social engineering. This was responsible for 11,589 fraud activities and this has made online fraud a growing concern for investors in financial services, (https://businessday.ng/editorial/article/ rising-cyber-fraud-in-nigeria-and-banks-losses/). Since Central Bank of Nigeria (CBN) in 2014 accelerated its effort to deepen cashless transactions, the rapidity of growth in electronic banking fraud has sustained.

According to Businessday editorial of 20th Feb. 2021, Nigeria Deposit Insurance Commission (NDIC) lamented that Nigerian financial system has been bedevilled by cyber-fraud that leads to heavy financial losses. For instance, in 2018, Nigerian banks lost over ₦15.5 billion ($41.6m), while ₦12.30 billion

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

was lost to various forms of frauds between 2014 and 2017. The most astonishing is that of all the financial service-related frauds, about 89 percent was perpetuated electronically, meaning that only 11 percent was non-electronic.

The pervasiveness of cybercrimes in Nigeria has led to the country being ranked **3rd** in global internet crimes behind UK and USA, (https://www.premiumtimesng.com/news/top-news/241160-nigeria-ranks-3rd-global-internet-crimes-behind-uk-u-s-ncc.hmtl). This, perhaps, justifies the country's position (**47th**) in Global Cybersecurity Index behind Mauritius, Tanzania and Ghana, (https://m.guardian.ng/technology/nigeria-lags-behind-mauritius-ghana-others-in-cybersecurity-ranking/amp/).

Results and Discussions

In tandem with majority of submissions above, it was found that although ownership and usage of phones and other related resources like social media platforms has increased exponentially, but digital penetration is still shallow, owing to digital divide that has left some people in the cool. This is exemplified by the number of respondents that are still computer illiterates. With this, 25.5% of those sampled are not Internet users and the level of ignorance is displayed by their lacking of the basic understanding of certain Internet jargons like phishing, spamming, cyber-fraud, as well as what constitutes cybercrimes. Furthermore, cybercrime as conceived by most of the respondents is all about fraud, perceived in the likes of conventional fraud (known in Nigerian parlance as "419"). This, to a large extent, affects how cybercrime is defined and the strategy that should be used in combating the menace. This is a problem that must be addressed because not all criminal activities on the net are about fraud.

The rate of cybercrimes as reported by the respondents is high (84%), and it is perpetrated mostly by unemployed graduates and students (50.5%), bank officials and their collaborators (40%) and other unspecified groups (9.5%). Just as the most prevalent crime is fraud (80%) with vishing (10%), spamming/hacking (7%) and all the three (3%) following in that order. It is found that those who engage their victims in bank fraud adopt modus operandi that involve sending business proposals to their potential victims and following it up with several fantastic, but non-existing offers, as well as sending of SMS with a threat of account closure should the account owner delay in supplying the needed personal information. In some instances, the "masked bank official" do volunteer to perform one or two functions for the client if they (clients) are too busy to visit the bank to correct errors noticed in their accounts by the "bank", and anyone who falls to their antics is duped.

In the face of all this, how are the authorities tackling the emerging challenges of cybercrimes? Answers were found from the responses provided by the respondents that for the police, they seem to be lacking in training/ cyber knowledge (28.5%); they are poorly remunerated and are corrupt (20.5%); they lack working tools like e-policing facilities (16.5%) and that cybercrimes law is not judiciously implemented (14.5%), while EFCC is failing for engaging in media trial without sufficient evidence to deal with suspects (20%). Above all, the police cannot work or prosecute anybody mostly as members of the public infrequently report incidence of cybercrime to the police or EFCC. The progress that would have been recorded is further punctured by the issue of job interference by a number of interest groups such as influential members of the society, hierarchy of security agencies, government officials, organisations, among others. Specifically, seventy-two percent (72%) of the respondents noted that the most worrisome is the duplication of duty by the Economic and Financial Crimes Commission (EFCC) and State Security Service (SSS) or Department of State Service (DSS) and Independent Corrupt Practices (and other related crimes) Commission (ICPC). It is also noticed that influential members of the public distort the operations of agencies on cybercrimes, and this is attested to by twelve percent of

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

the respondents (12%). In the same vein, people in government were fingered by sixteen percent of the respondents (16%) as usually interfering with the fight against cybercrimes.

Furthermore, irrespective of number of arrests made in Akwa Ibom State, security operatives are still found wanting in terms of acquisition of basic techniques needed for the investigation of this type of crimes as observed by the respondents. A concomitant of these problems is reflected on the number of serious cybercriminals caught and convicted. From the study, 67.5% of the respondents agreed that real and deadly cybercriminals are rarely caught. This, of course, is an indication that the courts and prisons would be ineffective in the fight against cybercrimes because of lack of inputs from the security agents. This is confirmed by the fact that offenders are rarely arraigned in the court as assented to by those sampled (60%). Majority of the respondents (80%) kicked against delay in prosecution of suspects and eventual release for want of adequate evidence. This, to them, indicates lack of intelligence required by cybercrimes.

With all this inaction on the part of government, individuals and organisations, the fallout is that economy (60%); national image and identity (10.5%); social / religious life (7.5%) are affected. Other respondents believe that all the three spheres of national life are affected (22%). Do we keep quiet and allow this to continue unabated? This is where the study becomes imperative and the respondents have not either accepted that the problems should be left just like that. Hence, various measures are suggested which include proper training of security agents; implementation of cybercrimes laws and filtering of the cyberspace to block infiltration and dubious acts. Other measures as suggested include the regulation of the cyberspace; adoption of proactive measures, provision of encryption facilities, stiffer penalties to deter commission of the crime, forensic and e-policing platforms; and mounting of campaigns to create public education and awareness.

Conclusion

The paper as designed, investigated, made findings and elucidated implications of cybercrimes as one of the correlates of economic crisis in Nigeria within situational crime prevention theory.

It is the view and the conclusion of the paper that as globalisation emerged through ICT revolutions, so also, are the latent implications including cybercrimes that excuse no country or individuals. Nigeria cannot be aloof by whatever guise in tackling this social malaise. Cybercrimes are high-tech and sophisticated crimes committed by intelligent criminals. Therefore, the country must arise in unison to fight it beyond the rhetoric that beclouds conventional crimes control patterns, because If it goes that analogue way, whatever gains made in other sectors will fritter away with a click of the mouse or buttons. Indeed, digital crimes beckon intelligence and digital preventive measures more than reactionary strategies.

Policy Implications

Containment of cybercrimes through SCP intervention

When conceptions of crime prevention lay the foundation in civil and other government regulations, it goes to affecting how government business, bureaucracies, products design and individual behaviour are regulated to reduce crime. This approach contrasts the traditional justice system model that seeks to arrest offenders one by one, (Mazerolle & Roehl, 1998).

While corroborating Clarke and Newman (2005a, 2005b) on how government regulation of crime, including virtual could be contained in any jurisdiction, some vital issues are espoused:

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.
Hosting by Research Parks All rights reserved.

- The role taken by government in any specific case depends on the options available, which vary with the crime, with the state of current technology, and with a host of other circumstances.
- The willingness of governments to intervene depends on their political complexion. The party in power, their ideology and political will, coupled with sincerity of purpose, which can markedly impinge on a country's use of regulatory power.
- Levels of concern about crime, which can vary considerably across countries, or in the same country over time, can strongly influence a government's willingness to intervene and regulate business practices. For example, Pease (2001) asserts that it was about the concern on car theft that prompted government of United Kingdom in 1992 to publish "league tables" of the most stolen cars in an effort to get manufacturers to improve their security. In Nigeria, if government is perturbed by the spate of financial fraud in the banking sector, it can impose heavy fines or other punitive measures on any bank that its cards or any facility was used in the act of hacking and illegal withdrawal of people's funds; government can as well deal with global system of mobile communications and internet service providers whose facilities like sim cards and sites serve as conduit in the act of defrauding people.
- The role of government depends on the system of government in place in the country concerned, its constitutional powers, and its relationship with the legal system.
- The laws and legal traditions in different countries can greatly affect the scope for government intervention. For instance, in the United States, there is a strong tradition of entrepreneurial lawyers filing class action liability suits on behalf of groups of citizens that have been harmed by the products or practices of business and industry. Therefore, if heavy penalties are imposed on convicted cybercriminals, and in addition, groups of victims take legal actions against them, the commission of cybercrimes may not look so appealing to other intended offenders.

Responsibility and competency

According to Newman, (2012) when crime is conceived in the likeness of pollution of any dimension, its regulation would be deepened and sustainable. The author suggested that for this to happen, **cap-and-trade approach** must be adopted, just as it is applied in controlling carbon emissions in industrialised climes. Crime-reduction trading assigns a monetary cost to organisation for failure to account for a specific crime that is not directly imposed by a third party, such as a government imposing fines, but is imposed by the offending business or entity primarily responsible for the criminal opportunity on itself as it engages in the marketplace. The cap-and-trade approach to control opportunities for crime created by businesses (as negative externalities of their doing business) requires those who are most competent to reduce opportunity for crime should bear the primary responsibility for its reduction, since they have the capacity to do so.

Here, Government can wield this same hammer on third party financial and cybersecurity managers such as Interswitch, Nigerian Communications Commission, the Central Bank, National Identity Management Commission and Nigerian Information Technology Development Agency (NITDA) for being ignorant and complacent in the protection and management of critical information infrastructure such as the Bank Verification Number (BVN), National Identity Number (NIN), Banks, among others. They should be fined heavily or made to refund to victims whenever they are duped or something sinister has happened since it is partly, their failure to secure the information super highway that has led to this breach.

Hardie and Hobbs (2005) offer that although, the relationship between competency and responsibility in

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

preventing crime is complex, but crimes like robbery, assault, or even murder, can be assessed by determining the entity or person that is most competent to prevent or reduce the specific crime. Most often, such entities are not necessarily the police, or even government.

This way of thinking about crime reduction also shifts the focus away from the traditional dispositional bias in policy making, which focuses on single cases; whether it is the deviance of individuals or corporations, and overly dependence on the criminal justice system or government regulation for its solutions.

To rely on agencies of criminal justice for crime reduction in the complex and rapidly changing world of crime, is an inadequate policy approach since it assumes that police and others in the criminal justice system have the competency to solve crime problems, even as the reality proves that the ravaging wave of crime, especially cybercrimes lie well beyond their resources or traditionally defined roles.

Against this backdrop, for containment to move beyond the usual grandiloquence, this study aligns with the advocacy of Freilich and Newman (2017) that those with greater competency to respond to crime should do it. This portends falling back on a wide range of institutions and organisations such as organised private sector (large and small), trade associations, unions, NGOs, interest groups and individuals, as well as government organisations, to solve specific problems of crime, but in this case, cybercrimes.

Further actions

- ✓ EFCC, DSS, NFIU, NCC and the Special Anti-fraud Unit of the Nigeria Police Force require more than physical means to combat cybercrimes. They need appropriate electronic devices, manned by forensic experts from diverse backgrounds to counter cybercrimes. Above all, everyone should be aware that successful cyber-attacks are testimonies of cybercriminals' high-level collaboration. To counter them, the available security architecture must be designed and implemented with collaborative efforts of all concerned to prevent the commission of cybercrimes in the first instance.
- ✓ Suspects should be processed through criminal justice system swiftly, and if found guilty, they should be visited with condign punishment. To achieve this, any law against cybercrimes should prescribe time frame for trial, and maximum punitive measures in commensurate with the weight of the crime to serve as a deterrent.
- ✓ Payment Service Providers (PSPs) must design and constantly review a formal security policy for internet payment services. Security objectives, risk appetite, roles and responsibilities, and a plan for the management of sensitive payment data should be well established.
- ✓ Any transaction initiated should have a prompter that alerts a customer on the status of such payment initiation before it is executed. Financial institutions or any payment system should confirm to their customers the payment initiation, and provide in good time, the information necessary to check that a payment transaction is carried out by the real owner of the account. Transaction monitoring mechanisms must be designed to prevent, detect and block fraudulent payment transactions. Where there are suspicious or high-risk transactions, they should be subject to specific screening and evaluation procedures.
- ✓ Constant and intensive public enlightenment and education are not only necessary, but imperative. Indeed, payment service providers have a duty to communicate with their customers in such a way as to reassure them of the authenticity of any messages received.

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

- ✓ Persons and organisations must refrain, and be careful on using ICT in an indiscreet manner. They must be careful with sensitive data including password to the system. There should be a limit to the number of log-in or authentication attempts; rules for internet payment services session "time out" should be defined, while time limits must be set for the validity of authentication.
- ✓ It is essential to ensure that all cyber traffics are routed through secured link SSL/HTTPS (Hyper Text Transfer Protocol Secured). Also, mobile users must be sure that the padlock icon has appeared on the web address bar, and they should double-check the SSL (Secure Socket Layer) certificates before logging-in sensitive data to avoid feeding an SSL proxy certificate that could lead to cyber-attack.
- ✓ For containment to move beyond rhetoric, these actions along with intervention techniques of SCP must be adopted and implemented faithfully.

References

1. Adepetun, A. (2020, July 9). Nigeria lags behind Mauritius, Ghana and others in cybersecurity ranking. *https://m.guardian.ng/technology/nigeria-lags-behind-mauritius-ghana-others-in-cybersecurity-ranking/amp/*.
2. Agency Report (2017, August 22). Nigeria ranks 3rd in global internet crimes behind UK, US - NCC. *https://www.premiumtimesng.com/news/top-news/241160-nigeria-ranks-3rd- global-internet-crimes-behind-uk-u-s-ncc. Hmtl*.
3. Akosile, A. (2005, November 18). $242M scam: Nwude pleads guilty, bags 25 yrs. jail term. In *This Day Newspaper* (Nigeria), p. 25.
4. Anonymous (2021, February 22). Editorial: Rising cyber fraud in Nigeria and banks' losses. *https://businessday.ng/editorial/article/ rising-cyber-fraud-in-nigeria-and-banks-losses/*.
5. Awak, E. U. (2019a). Threats of cybercrimes in Nigeria and the theoretical disposition of RAT (Routine Activity Theory). *CEKA International Journal of Social Sciences & Organisational Behaviour*, *7*(2).
6. Awak, E. U. (2019b). The role of the family and educational institutions in curbing social vices in Nigeria. *AKWAPOLY Journal of Communication and Scientific Research, 4*(1).
7. Awe, O. (2006, January 4). Cyber fraud leads to blockage of Nigeria's IP address. In *The Punch Newspaper* (Nigeria), p. 31.
8. Bowers, K., & Johnson, S. (2005). Using publicity for preventive purposes. In N. Tilley (Ed.), *Handbook of Crime Prevention and Community Safety*. Willan Publishing.
9. Braga, A., & Kennedy, D. (2012). Linking situational crime prevention and focused deterrence strategies. In N. Tilley & G. Farrell (Eds.), *The reasoning criminologist: Essays in honor of Ronald V. Clarke*. Routledge.
10. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime policing. *An International Journal of Police Strategies and Management, 29*(2), 408-433.

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

11. Clarke, R. V. G. (1999). *Hot products: Understanding, anticipating and reducing the demand forstolen goods*. Police Research Series, 98. Home Office.

12. Clarke, R. V. G., & Goldstein, H. (2003). Thefts from cars in center-city parking facilities: A case study in implementing problem-oriented policing. *Crime Prevention Studies, 15*, 257-298.

13. Clarke, R. V. G., & Newman, G. R. (2005a). Modifying criminogenic products: What role for government? In R. V. G. Clarke & G. R. Newman (Eds.), *Designing out crime from products and systems*. *Crime Prevention Studies, Vol. 18*. Willan Publishing.

14. Clarke, R. V. G., & Newman, G. R. (Eds.). (2005b). *Designing out crime from products and systems*. *Crime Prevention Studies, Vol. 18*. Willan Publishing.

15. Comer, D. (2006). The Internet Book. *Prentice Hall.*

16. Eck, J. E., & Madensen, T. (2012). Situational crime prevention makes problem-oriented policing work: The importance of interdependent theories for effective policing. In N. Tilley & G. Farrell (Eds.), *The reasoning criminologist: Essays in honour of Ronald V. Clarke* (Crime Science Series). Routledge.

17. Ekblom, P. (2012a). Happy returns: Ideas brought back from situational crime prevention's exploration of design against crime. In N. Tilley & G. Farrell (Eds.), *The reasoning criminologist: Essays in honour of Ronald V. Clarke*. Routledge.

18. Ekblom, P. (Ed.). (2012b). Design against crime: Crime proofing everyday products. *Crime Prevention Studies, Vol. 27*. Lynne Rienner Publishers.

19. Edelson, E. (2003). The 419 scam: Information warfare on the spam front and a proposal for local filtering. *Computers & Security, 22*(5), 392-401.

20. Felson, M. (2008). Routine activity approach. In R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis,* 70-77. Willan Publishing.

21. Freilich, J. D., & Newman, G. R. (2016). Transforming piecemeal social engineering into "grand" crime prevention policy: Toward a new criminology of social control. *Journal of Criminal Law and Criminology, 105*(1), 209-238.

22. Freilich, J. D., & Newman, G. R. (2017). Situational crime prevention. https://doi.org/10.1093/acrefore/9780190264079.013.3

23. Froehling, O. (1997). The cyberspace war of ink and Internet in Chiapas. *The Geographical Review, 87*, 291-307.

24. Fuller, J. R. (2005). *Criminal Justice: Mainstream and Crosscurrents*. Prentice Hall.

25. Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Addison Wesley.

26. Gantz, J., & Rochester, J. B. (2005). Pirates of the Millennium. *Prentice Hall.*

27. Gehring, V. V. (2004). The Internet in Public Life. *Rowman and Littlefield.*

28. Goodin, D. (2008). Fake subpoenas harpoon 2,100 corporate fat cats. *The Register.* http://www.theregister.co.uk

29. Goodman, M. D. (2001). Making computer crime count. *FBI Law Enforcement Bulletin, 27*, 31-42.

30. Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*, 243-9.

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.

31. Hardie, J., & Hobbs, B. (2005). Partners against crime- the role of the corporate sector in tacking crime. *Crime Prevention Studies*, *18*, 85-140.
32. Hollinger, R. (1988). Computer hackers follow a Guttman-like progression. *Social Sciences Review*, *72*, 199-200.
33. Joseph, J. (2003). Cyberstalking: An International Perspective. In Y. Jewkes (Ed.) *Dot.cons:Crime, Deviance and Identity on the Internet.* Willan Press.
34. Koziol, J. (2003). *Intrusion Detection with Snort*. Sams Publishing.
35. Krebs, B. (2006). Flaws in financial sites aid scammers. *Security Fix*. http://blog.washingtonpost.com/securityfix
36. Marshall, J. A. (1999). Internet crimes encountered by novice surfers. *Journal of Industrial Technology, 15*(2), 1-5.
37. Mazerolle, L. G., & Roehl, J. (Eds.). (1998). *Crime prevention studies, Vol.* 9. Special Issue on Civil Remedies and Crime Prevention. Criminal Justice Press.
38. Newman, G. R. (2012). Designing markets for crime reduction. *Crime Prevention Studies, 27*, 87–106.
39. Rehmeyer, J. J. (2007). Mapping a medusa: The internet spreads its tentacles. *Science News*, *Vol.171*, 15.
40. Olokor, F., & Okere, A. (2021, August 29). Thisday disowns fake publication on Uzodinma, seeks culprit's arrest. https://punchng.com/thisday-disowns-fake-publication-on-uzodinma-seeks- culprits-arrest/
41. Pease, K. (2001). *Cracking crime through design*. Design Council.
42. Smith, A. D. & Rupp, W. T. (2002). Issues in cybersecurity: Understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security,10*(4),178-183.
43. Snail, S. (2009). Cybercrime in South Africa–hacking, cracking, and other unlawful online activities. *Journal of Information, Law & Technology (JILT)*, *1*, 89-96.
44. Turkle, S. (1995). *Life on the Screen: Identity in the Age of the Internet*. Simon & Schuster.
45. Ukoka, L., & Awak, E. U. (2016). *Professional ethics & social responsibility: The social construction of consciousness for professionals and* society. Anikzo Global Ventures.
46. Ukoka, L., & Awak, E. U. (2015). *Contemporary research methodologies*. Anikzo Global Ventures.
47. Wall, D. S. (2006). *Cybercrimes*. Polity Press.
48. Wall, D. S. (2003). Mapping out cybercrimes in a cyberspatial surveillant assemblage. In F. Webster and K. Ball (Eds.), *The Intensification of Surveillance: Crime Terrorism and Warfare in the Information Age*, 112-136. Pluto Press.
49. Wall, D. S. (2001). Cybercrimes and the Internet. In D. Wall (Ed.), *Crime and the Internet*. Routledge.
50. Yar, M. (2006). C*ybercrime and society*. Sage.

E-mail address: info@researchparks.org
Peer review under responsibility of Emil Kaburuan.