VIVIFICATION AND ADAPTABILITY OF ROUTINE ACTIVITY THEORY (RAT): A PARADIGMATIC APPROACH TO DETERRING CYBERCRIMES IN NIGERIA

Emmanuel U. Awak, PhD

Department of General Studies,
Akwa Ibom State Polytechnic, Ikot Osurua, Nigeria
emmanuel.awak@akwaibompoly.edu.ng
https://orcid.org/0009-0003-8926-0975

Abstract

Internet, with its anonymity has created a platform where e-fraud, cyberterrorism, hacking and other cybercrimes thrive. The ill-implementation of legislation targeting cybercrimes; lack of virtual evidence, knowledge of investigation, and theorisation have continued to negate effective policing of the cyberspace. Some contemporary discourses portend qualitative similitude of cybercrime and 'terrestrial crime', while conjecturing explications radiate within the confines of grand theories of crime causation. Conversely, this paper adopts a descriptive method of analysis, where materials were gathered through secondary sources to explore and vivify Routine activity theory and the extent to which its perspectives and aetiological schema can be transposed to crimes committed in a 'virtual' environment. The parameters of cybercrime are analysed as a security concern, while it is concluded that the strands of the theory are very descriptive of the ravaging landscape of these crimes. Indeed, since it has been discovered in the study that the prevalence of cybercrimes annihilates germane quest for sustainable security and development, utilisation of data surveillance technologies, computer literacy and cybercrime awareness campaign, legislation, intelligence policing and co-operation among stakeholders are advocated as adaptive measures to truncate and wane the scourge of cybercrimes.

Keywords: Cybercrimes, Internet, RAT, Vivification, Virtual

1.0 Introduction

Cybercrimes are any illegal acts committed within a computer network or facilitated by the use of a computer or electronic system, (Comer, 2006 in Awak, 2019). Some of the variants range from hacking, phishing, vishing, password sniffing, web cramming, spoofing, credit card fraud to identity theft. Others involve data kidnapping through industrial espionage, software piracy, cyber and financial fraud, stocks manipulation or fraudulent business deals, as well as computer sabotage and cyber terrorism, (Awak, 2019). Infact, Wall (2001 in Awak, 2019) 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 like a common event 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, 2019). This explains why the Nigeria Army in 2020 left its constitutional duties to join in countering cybercrimes before the #EndSARS protestations disrupted the operation, (Awak, 2022).

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, (Yar, 2006 in Awak, 2022). However, in Nigeria, it took the federal government over fifteen (15) years to enact a law on cybercrimes (Prohibition, Prevention, etc.) Act (2015), after it set up the Nigeria Cyber Working Group (NCWG) in 2000 (Awak, 2022) and the amended version of 2019 by the Nigerian government; though the implementation and policy direction are matters of grave concern.

That the spate of cybercrimes and the inadequacy of safety measures to police the system and its processes are manifest in the geometric number of those enlisted into cybercriminal gangs; however, this does not negate the exponential rate at which ICTs and their applications have spread (Awak, 2022). Certainly, financial, psychological, political and economic losses recorded through cybercrimes are deleterious to Nigeria's economy and overall well-being. Yet, the larger population is stuck in ignorance, digital divide, inequality and inaccessibility to critical ICTs infrastructure. This population is vulnerable, and often, victims of various antics of those lurking around the net.

Irrespective of existing measures to counter cybercrimes, the financial, economic and social fabric of Nigerian society are stultified unabated by activities of cybercriminals, thereby, enunciating adaptability by RAT as a paradigmatic approach in the invention and implementation of stringent measures to curb strangulating pangs of cybercrimes in the country.

As cited in Awak (2022), NIBSS lamented that between July and September, 2019, Nigerian banks lost N552million to fraud related transactions, but as a result of the Covid-19 pandemic and subsequent lockdown in 2020, the loss astronomically peaked at N3.5billion 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 N410 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. Today, many developed countries are grappling with Ransomware attacks that seem like fairy-tale to Nigerians and it is worrisome that if such countries like the USA, Britain, among others with all cyber security architecture in place are made to swallow a disruption cost of up to $20b a year, then, when Nigeria becomes aware of the attacks, the cost surely, would be disastrous.

According to Chainalysis, a software company, "Gangs of ransomware hackers made more than $350m in 2020, a 311 per cent jump on the previous year, (Murphy in Financial Times, 2021, P. 6). In ransomware attacks, data and other internet resources are kidnapped and ransom demanded. It is the cyber version of conventional kidnapping that is rampant in Nigeria.

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/) (cited in Awak, 2022). 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. Hypnotism, ritualisation and social engineering have become veritable tools in the hands of cybercriminals, and explain the apathy towards cashless system as

displayed by the people between January 31 and March 5, 2023 when cash crunch made cashless facilities palpable. That Nigerians craved for cash was a consequence of lack of trust in the mobile banking or cashless policy and a serious damage to the economy.

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 N15.5 billion ($41.6m), while N12.30 billion 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, (Awak, 2022).

The pervasiveness of cybercrimes in Nigeria 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/) (cited in Awak, 2022; Adepetun, 2020). It is also, estimated that financial loss at the global scale by 2025 will not go below $10.5 trillion with daily cybercrime cases optimising at 2,328.

The scourge of cybercrimes is therefore, reflected in the humongous recoveries by EFCC. For instance, between October 2023 and September 2024, 3,455 convictions were secured, while #248,750 billion, $105,423million, $180,300, £53,133.64; €172,547.10 and T1,300.00 IndianRupees, CAD$3,400.00, ¥74,859.00 Chinese Yuan; AUS$ 740,00, 170.00 UAE Dirham, 73,000.00 Korean WO N, CFA7,821,375.00 and R50,000 South African Rands (www.noa.gov.ng/thechangingfaceofanti-corruptionwar).

Indeed, cyber criminals around the world lurk on the net as ever-pervading menace to the financial and economic health of the society, which has provoked growing interests to investigate multisectoral domains of cybercrimes.

2.0 Conceptual Clarifications

2.1 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 account.

2.2 Fraud: Computer fraud is any dishonest misrepresentation of fact intended to induce another to do or refrain from doing something which causes loss. 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 in Awak, 2019).

2.3 Software piracy: It has to do with theft of software through illegal copying of genuine programmes or the counterfeiting and distribution of products intended to pass for the original. Piracy describes a significant range of activities, of which, most are unlawful. It involves "…make or making use of or reproducing the work of another without authorisation" (Craig, Honick, & Burnett, 2005, p. 12).

2.4 Email bombing: Email bombing has to do with sending a large number of emails to the victim, which results in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing (Goodin, 2008).

2.5 Harassment: Harassment, to Philippsohn (2001), directs obscenities and derogatory comments at specific individuals focusing for example, on gender, race, religion, nationality, sexual orientation, among others.

2.6 Cyber-terrorism: A cyberterrorist is someone who intimidates or coerces a government or organisation to advance his or her political or social objectives by launching computer-based attack against computers, network and the information stored on them (Comer, 2006). On the other hand, Cyberterrorism is an act of terrorism committed through the use of cyberspace or computer resources (Gordon & Ford, 2004 in Awak, 2022). There are also hacking activities organised by groups within networks and directed towards individuals and families, with a view to causing fear among the people. Terrorists may demonstrate their ICT power by collecting information relevant for ruining peoples' lives through act of robberies, blackmailing, stalking, among others (Wall, 2011).

2.7 Hacking/cracking: This means an illegal intrusion into a computer system and/network. It is a process whereby one uses one's programming abilities to design various programmes with malicious intent to gain unauthorised access to a computer or network. For instance, a hacker could insert a pornographic content just to embarrass the participants of a zoom meeting.

2.8 Virus dissemination: Viruses are programmes that attach themselves to a computer or a file and then circulate themselves to other files and to other computers. They usually affect the data on a computer, either by altering or deleting it. However, Worms merely make functional copies of themselves repeatedly until they eat up all the available space on a computer's memory. Examples of malicious software worms that destroy the system of the victim include Trojan horse, Time bomb, Logic bomb, Rabbit and Bacterium (Awak, 2019).

2.9 Internet time thefts and card cloning: These 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 (ISP) or even global mobile system of communication (GSM). Other cases involve card cloning aided by the installation of fake ATM fingerplates, card reader overlays, hidden cameras and PIN-capture overlays, as well as, dummy keypad to record and capture PIN numbers as they are entered.

2.10 E-mail address spoofing: The sender information shown in e-mails (the "From" field) can be spoofed easily. This technique is commonly used by Spammers to hide the origin of their e-mails and could lead to problems such as misdirected bounces (i.e. e-mail spam backscatter). E-mail address spoofing is done in quite the same way as in writing a forged return address using snail-mail. As long as the letter fits the protocol, (i.e. Stamp and postal code) the SMTP protocol will send the message (Joseph, 2003 in Awak, 2019).

2.11 Victims: Victims of computer or cybercrime include the person and the property of an individual, group of individuals, government, firm, company and communities, rural/urban centres, regions, countries and continents.

3.0 Methodology

Qualitative research approach was utilised in the course of this study since it is an open and emerging approach (Crasswell, 1998 in Awak, 2022). Corroborating Struwig and Stead (2001), it is expedient to examine this topic

within qualitative approach, because previous researches on the subject matter are capable of influencing the understanding of events and context of the present study. Therefore, data were derived from secondary sources to navigate the blooming landscape of cybercrimes in Nigeria and the adaptability of approaches of Routine activity theory in the quest to deterring the scourges.

4.0 Review of Related Literature

It is unfathomable and alarming when the speed, spate and frequency of commission of crimes become so ingrained in the socio-political and economic life of a nation. This is why Awe (2006 in Awak, 2011) 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 in Awak, 2011), 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 as the moral fabrics and conscience collective of families and societies are not spared, (Awak, 2022). Again, 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, 2022, 2011).

The Internet has created a cybercrime-fraud platform where multifarious types of fraud are committed over computer networks, making effective policing almost impossible.

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 (Awak, 2019).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 in Awak, 2011). On 3rd August, 2000, Canadian federal prosecutors charged Mafia Boy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for attacks on Amazon.com, eBay, Dell Computer, Outlaw.net, and Yahoo. Mafia Boy had also attacked other websites (Krebs, 2006 in Awak, 2019). Hacking or gaining unauthorised access to a computer system, programmes or data, opens a broad field for inflicting damage (Rehmeyer, 2007).

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. They 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.

Appreciating the magnitude of this problem, as well as devising possible containment strategies underscores the essence for theorisation.

5.0 Theoretical Stance: Routine Activity Theory (RAT): Lawrence Cohen and Marcus Felson (1979)

Routine activity theorists posit that crime is normal and depends on the opportunities available. If a target is not protected enough, and if the reward is worth it, crime will happen. Crime does not need hardened offenders, super-predators, convicted felons or wicked people. Crime just needs an opportunity, (Birkbeck, & Lafree, 1993 in Awak, 2019). Crime is neither spectacular nor dramatic. It is mundane and happens all the time (Bennett, 1991in Awak, 2019).

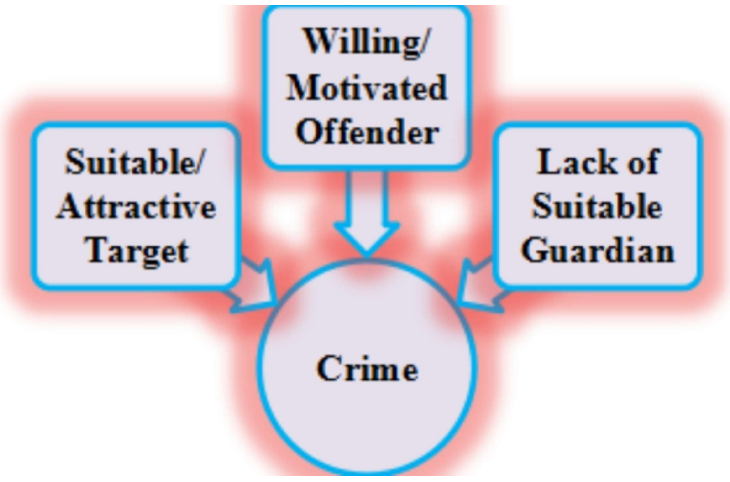
Again, crime is relatively unaffected by social causes such as poverty, inequality, unemployment, (Cohen, Kluegel, & Land, 1981 in Awak, 2019). This is explained by the fact that most of the developed countries are equally caught in the web of crimes (including cybercrimes) just as the developing countries.

According to Felson and Cohen (1979), this is because the prosperity of contemporary society offers so much opportunities of crime that is, there is much more to steal and it is much easier to carry it out through the net.

Though Routine activity theory is controversial among sociologists who believe in the social causations of crime, but several types of crime explained in the theory including copyright infringement, cybercrime, employee theft, and corporate crime has justified its existence (Bernburg, &Thorlindsson, 2001). This is because the theory provides a simple and powerful insight into causes and threats of crimes. At its heart is the idea that in the absence of effective controls, offenders will prey upon attractive targets. To have a crime, a motivated offender must come to the same place as an attractive target. For property crimes, the target is a thing or an object (Cohen, & Land, 1980 in Awak, 2019). For personal crimes, the target is a person. If an attractive target is never in the same place so as to motivate offender, the target will not be taken, damaged, or assaulted (with exception to cybercrimes and frauds). Also, there are controllers, whose presence can prevent crime. If the controllers are absent, or present, but powerless in terms of knowledge, working tools, among other crime prevention necessities, crime is possible.

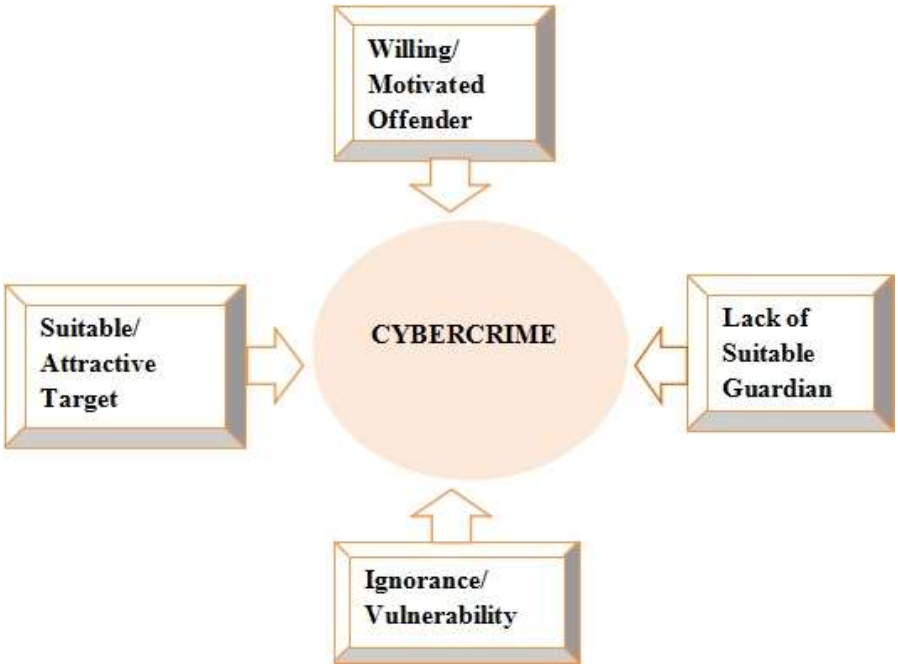
The strands of the theory is summarised as follows:
According to the theory, three things happen at the same time and in the same space before a crime takes place:

- A suitable target is available;
- there is the lack of a suitable guardian to prevent the crime from happening; and
- a likely and motivated offender is present.



Source: Modified version of Felson and Cohen, 1979 in Awak, 2019

Fig. 2: Process of cybercrime causation



Source: Awak, 2024

An analysis of each of these scenarios unveils the following:

(a) **An attractive/ suitable target:** The first condition for any crime to occur is that a suitable target must be available. There are three major categories of target. A target can either be a person, an object or a place. The qualities of the targets include *availability, visibility, accessibility, removability, disposability, valuable, inertia, concealable*, and *enjoyable*. Furthermore, no matter how suitable a target is, an offence will not occur unless a capable guardian is absent and a likely offender is present. Infact, the *social situations* in which actors find themselves mediate decisions about whether or not they will act on their inclinations (Yar, 2005 in Awak, 2022).

(b) **Absence of a capable guardian:** The capable guardian whose presence would discourage a crime from taking place must be absent. A capable guardian has a 'human element', that is usually a person whose mere presence would deter potential offenders from perpetrating an act. A

capable guardian could also include electronic monitoring devices such as Close Circuit Television (CCTV), Internet surveillance device and other intelligence devices, provided that someone is monitoring it at the other end of the camera. Other capable guardians are police patrols, security guards, neighbourhood vigilantes, doorstaff, vigilant staff and co-workers, friends, and neighbours (Awak, 2022).

Some of the guardians are formal and deliberate, like security guards; some are informal and inadvertent, such as neighbours, parents, teachers, peers and others. A target with an effective guardian is less likely to be attacked by a potential offender than a target without a guardian. If the guardian is absent, weak or corrupt, little protection is provided to the target. It is also, possible for a guardian to be present, but ineffective (Miethe & Meier, 1990 in Awak, 2019). For example, a CCTV camera is not a capable guardian if it is set up or sited wrongly. Staff might be present in a cyber café or shop, agencies of criminal justice such as the police without sufficient training, cyber intelligence or awareness to be an effective deterrent.

(c) **Willing/motivated offenders:** When a suitable target is unprotected by a capable guardian, there is a chance that crime will take place. The final element in this picture is that a likely offender has to be present. RAT looks at crime from an offender's point of view. A crime will only be committed if a likely offender thinks that a target is suitable and a capable guardian is absent and that there is a knowledge lacuna by the owner of the target. It is their assessment of a situation that determines whether a crime will take place or would be deferred (Awak, 2022; Grabosky, 2001).

(d) **Ignorance/ vulnerability:** Crime will occur when the motivated offender is convinced that the owner of the attractive target is ignorant or vulnerable to the antics of offender. For instance, lack of ICT knowledge, inability to read and write, willingness to accept "audio" business proposal and over-trust or confidence in a third party whereby they become privy to security codes or PIN. The emerging twist of ritualisation of the net where victims are believed to be hypnotised and excessive greediness add to dimensions of vulnerability.

5.1 Operational tools

It must be stated that all of the people in this theory use tools to help accomplish their criminal or crime control objectives. Tools that gang members use may include books, guns, flashdrives, laptops, computer, cyberspace, phones and cars. Offenders without access to tools are less likely to be able to escape handlers, enter unauthorised places, and overcome targets or victims, guardians, and managers. Guardians may use light to increase surveillance, engraving devices to mark property, and legislation to help reduce the chances of victimisation. Place managers can use gates, fences, cybersecurity, close circuit devices, signs and other tools to regulate conduct. With effective tools, handlers, victims, guardians, and managers will have a greater chance of keeping crimes from occurring. The tools used are often highly specific to the crime in question. The tools an offender needs for a burglary (e.g., a screw driver, machete, axe, among others) are likely to be different from those needed for a robbery (e.g., a gun, knife, hammer, and others) and virtual equipment needed for cybercrimes.

However, in this respect, at least, the challenge to formal guardianship presented by cyberspace is only a more intensified version of the policing problem in the terrestrial world; as Felson (1998, p. 53) noted, "The police are very unlikely to be on the spot when a crime occurs." In cyberspace, as in the terrestrial world, it is often only when private and informal attempts at effective guardianship fail that the assistance of formal agencies is sought, (Grabosky, & Smith, 2001).

Routine Activity theory and its modus operandi are very relevant to the present paper. It has proved that if the offenders are well guarded such that little opportunity occurs for crimes, the society would be better for it. It goes further to show that if the agencies of criminal justice are properly trained, managers of cyber café are alert, neighbours, enterprises and neighbourhood are united against any dimension of cybercrimes that the scourge could be deterred. Indeed, a paradigm shift in containment approaches and adaptability to the currency of the time is apt and compelling.

6.0 Adaptability and Paradigmatic Approach

a) The cost of prosecution, the discretion of the prosecutor and the implementation of the extant laws are often called to question. Prevention, closure of opportunity and removal of targets, along with problem-solving policing innovate policing culture of security agencies.

b) The application of cap-and-trade approach is very innovative and a novel strategy aimed at reducing cybercrimes. By this approach, crime-reduction assigns a monetary cost to organisation for failure to take proactive action for a specific crime. Here, Nigerian Communications Commission, global systems of mobile communication (service providers), banks and any other financial or business institutions, whose platforms were used in the commission of crimes shall pay heavy fines or made to refund to victims of cybercrimes whenever they are duped since it is their failure to secure the information high way that led to such a breach. The study pushes for a legislation and implementation of this policy.

c) De-radicalisation exercise discourages enlistment into cybercriminal gangs.

d) Establishment of ICTs centres, provision of counselling services and life-skills trainings can facilitate adaption and compliance, as well as innovate the cultural, attitudinal and perceptual constructs of the people.

e) Avoiding the use of O.MG cables is non-negotiable. Stealth as one of the features of OMG cables aligns most with the concepts of adaptability and pragmatic approach. This is because the implant is reputed to staying dormant until a payload is deployed. It does not require any logs or detections. It behaves like a normal USB 2.0 cable with 5v charging, 480mps data transfer spoof of any USB identifier (VID/PID), extended USB identifier and network MAC address.

The Elite models contain a passive hardware keylogger designed for FullSpeed USB keyboards with detachable cables. It can store up to 650,000 keystrokes.

Fig. 3: Samples of O.MG cables

Photo credit: Thenationthailand.com

Photo credit: Google.com

According to the Nationsthailand Newspaper, "Oh my God" (OMG) was developed by Mike Glover. The cable is meant for charging of phones. Besides this, it has the capability that allows hackers to gain unauthorised access to any device it is plugged into, and would usually grant access to open applications, steals passwords or download viruses or malware of the device it is plugged in. Its popularity and wide usage is thwarted by high cost since not everyone can afford a cable sold at about $180.00. However, irrespective of its high cost, acquisitions are mostly done by high profile targets.

7.0 Conclusion

The effort of this paper has been to investigate and discuss the findings of emerging criminal problems that are posing new challenges to the government, public, agencies of criminal justice and indeed, all people, and placed it within a theoretical anchorage for better elucidation.

It is the view and the conclusion of the paper that as globalisation is brought about by the ICT revolutions, so also, are the latent implications including cybercrimes that excuse no country or individuals. Cybercrimes are high-tech and sophisticated crimes committed by intelligent criminals and as such, deterrent can be achieved with sophisticated stringent measures, faithful implementation of all extant rules, superb cybersecurity intelligence and denial of opportunities for cybercrimes to flourish.

8.0 Recommendations

- Culprits when caught should be tried without delay and if found guilty, they should be swiftly visited with condign punishment. To achieve this, Cybercrimes (Prohibition, Prevention, etc.) Act (2015), Amendment Act (2024) and similar legislations must be implemented to the letter, irrespective of who is involved.
- Public enlightenment to understand and effect necessary actions on the three P's (phishing, patches and passwords) of cybercrimes.
- Social media platforms, content providers and cyber cafes must be censored and monitored where those abetting cybercrimes should be arrested and prosecuted or even close down.
- Every person and organisation must take personal responsibility to protect by refraining from acts that are capable of making them vulnerable to attack and susceptible to manipulation by cybercriminals. They must be careful with the passwords, PINs, codes to the system and other mobile applications, just as installation of strong anti-virus software in the system and regular update and other cybersecurity measures are important.
- Enterprise security measures such as communication, coordination and collaboration must be designed to align with industrial cyber security needs.
- It is not advisable to login passwords and other details on the net especially when the site is strange to the user. It should be noted that any web address with "***http://***" is questionable and any login could be easily manipulated for some sinister activities because it provides no security. However, an address with "***https://***" is a secure address.
- The best data and information protection is to avoid connecting to suspicious Wi-Fi networks or using any charging cables found idling around someone's table or office or room.
- Users of ATM should be aware of the print-out receipt and details of their account in order to forestall any cloning of their cards that could result in loss of heavy amount of money.
- Bridging digital divide should be targeted with aggression.

References

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/*.

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/.*

Awak, E. U. (2022). Cybercrimes and economic crisis in Nigeria: Essentialising containment beyond the rhetoric. *International Journal on Economics, Finance and Sustainable Development*, *4*(6), 121-136.

Awak, E. U. (2019). Threats of cybercrimes in Nigeria and the theoretical disposition of RAT (Routine Activity Theory). *CEKA International Journal of Social Sciences & Organisational Behaviour*, *7*(2).

Awak, E. U. (2011). The police and cybercrimes control in Nigeria. *PhD dissertation*, University of Uyo.

Bernburg, J. G., & Thorlindsson, T. (2001). Routine activities in social context: A closer look at the role of opportunity in deviant behaviour. *Justice Quarterly, 18*, 543-67.

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.

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.

Clarke, R., & Felson, M., Eds. (1993). *Routine Activity and Rational Choice*. Transaction Press.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Cohen, L., Kluegel, J., & Land, K. (1981). Social inequality and predatory criminal victimization: An exposition and a test of a formal theory. *American Sociological Review,* 46:505-24.

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.

Felson, M. (1998). *Crime and everyday life* (2nd Edition.). Pine Forge Press.

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

Joseph, J. (2003). Cyberstalking: An international perspective. In Y. Jewkes (Ed.) *Dot.cons: Crime, Deviance and Identity on the Internet*. Willan Press.

Murphy, H. (2021, February 18). Cybercrime: Negotiators cut deals with ransomware gangs. *Financial Times*.

Premium Times Newspaper (Nigeria) (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*.

Rehmeyer, J. J. (2007). Mapping a medusa: The internet spreads its tentacles. *Science News*, *Vol.171*, 15.

Siegel, L. T. (2006). *Criminology*, 9th Edition. Thomson Wadsworth.

Snail, S. (2009). Cybercrime in South Africa–hacking, cracking, and other unlawful online activities. *Journal of Information, Law & Technology (JILT)*, 1:89-96.

The Nations (2022, October 10). *O.MG cables*. nationthailand.com.

Wall, D. S. (2006). *Cybercrimes*. Polity Press.

Yar, M. (2006). C*ybercrime and society*. Sage.