COUNTER MEASURES AGAINST CYBER-INSECURITY: COLLABORATIVE SOLUTIONS WITH ETHICAL HACKERS, THE UNITED KINGDOM APPROACH

OBINNE OBIEFUNA, PhD*

Abstract

The status quo in global cyber insecurity is unacceptable. Despite various measures to stem the tide of cybercrime, cybercrime is on the increase globally. In Africa, Nigeria ranks among the highest countries in Cyber insecurity and this dismal statistics has adversely affected her stature in the international sphere. Foreign direct investment has taken a nosedive as international businesses prefer South Africa and Ghana to Nigeria in business negotiation, technology transfer and foreign aid. This repercussion for cybercrime has stunted Nigeria's economic growth. Accordingly, legislative solutions have been adopted. The Cybercrime Prohibition Prevention Act 2015 CPPA was passed by the Nigerian Parliament to curb cybercrime within her jurisdiction. This Act has been arguably less than effective as Nigeria is a hot spot for cybercrime. Nigeria has also invested a lot of effort in the training of law enforcement officers (LEAS) in order to tackle this high tech crime. In this article, we question the conventional approach of fighting cybercrime. We argue that different method to eradicating cybercrime should be adopted as the current approach has been grossly effective. Using comparative evaluation, the article examines the roles of ethical hackers in curbing cyber criminality. It identifies the immense benefits that tackling this crime from this approach confers as seen in the United Kingdom. The article finds that custodial sentences merely stigmatize and harden these convicted cybercriminals. It is suggested that the approach of enlisting cybercriminals to use their expertise in information technology to help tackle this sophisticated crime will help to greatly reduce if not eradicate cyber criminality in Nigeria.

* PhD (Nig) LLM(Essex), LL.B (Nig) BL, Lecturer, Department of International and Comparative Law, Faculty of Law, University of Nigeria Email: obinneobiefuna@gmail.com

Keywords: Cyber crime, Ethical hackers, United Kingdom Approach, Cyber insecurity

1. Introduction

The internet invented by the US defence department in the twentieth century has become the most influential and the most far reaching communications breakthrough in history[1]. It's a marvel how the world coped without it.[2] The modern internet remains a backbone for critical infrastructure around the world. It is the main artery of global digital trade.[3] Almost all spheres of modern life is dependent on the Internet; research, the global digital economy, democracy and national security now completely depend upon the stability and security of cyberspace.[4] Statistics show that roughly 5.7 billion people use the internet every day;[5] there is estimation that there will be more than 7.5 billion internet users in 2030. With this increased internet use there was equally increased use of the same internet as a playground for criminals.[6] Malignant users of cyberspace commit heinous crimes online. Cybercriminals are becoming more emboldened and atrocities committed on the World Wide Web are catastrophic. Cybercrime has hit the globe so hard that the net profit from this crime is projected at

---

[1]Katie Hefner, Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York :Simon And Schuster Paperbacks 1996) 2

[2]A. G. Blanco, "The Impact of COVID-19 on the Spread Of Cybercrime," BBVA, 27 04 2020.https://www.bbva.com/en/the-impact-of-covid-19-on-the-spread-of-cybercrime accessed 4 May 2023

[3]Council on Foreign Relations, Confronting reality in cyberspace <https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace/download/pdf/202207/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf> accessed 7 January 2023.

[4] Sohail Razan Chohan Guangwei Hu Strengthening Digital Inclusion Through E-Government: Cohesive ICT Training Programs To Intensify Digital Competency [2020] *Information Technology for Development,* (28) (1) 16-38

[5] Jason Wise, How Many People Use The Internet Daily In 2023 April 10 2023< https://earthweb.com/how-many-people-use-the-internet-daily> accessed 7 May 2023

[6] NI Alli & others Cybercrime An Emerging Challenge For Internet Users :An Overview,[2018] (50) (3D*) Sindh University Research Journal (Science Series)* 55

$10.5 trillion USD annually by 2025.[7] The potential total loss has grown from $6.9 billion in 2021 to more than $10.2 billion in 2022.[8] Furthermore IBM executive chairman Ginny Rometti while sharing her opinion on the seriousness of cybercrime opined;

> We believe that data is the phenomenon of our time, it is the world's new natural resource and it is transforming every profession and industry. If all of this is true then cybercrime, by definition, is the greatest threat to every profession, every industry, and every company in the world.[9]

Considering the magnitude of this global threat, Companies under pressure to protect their networked devices from cybercriminals invested more than $1 trillion on global cybersecurity products and services.[10] Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed 13.82 trillion dollars in 2028.[11]

Notwithstanding these huge financial investments to ensure a crime proof cyberspace, cyber attacks are growing exponentially. In a bid to curb this menace, governments using traditional means of fighting crime have enacted legislation both regionally and otherwise to tackle cybercrime; for example in England the Computer Misuse Act Of

---

[7] Steve Morgan, Cybercrime to Cost the World $10.5 Trillion Annually By 2025 November 13, 2020 <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ > accessed 7 May 2023

[8] Federal Bureau Of Investigation, Internet Crime report 2022 <https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf> accessed 7 May 2023

[9] Sofia said Birch, IBM's CEO on hackers: "Cyber crime is the greatest threat to every company in the world November 26 2015<https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/> accessed 6 April 2023

[10] Md Haris Uddin Sharif, Mehmood Ali Mohammed, A Literature Review Of Financial Losses Statistics For Cyber Security And Future [2022]*Trend world Journal Of Advanced Research And Reviews,* 15 (1)139

[11] Ani Petrosyan, Estimate Cost from Cybersecurity Worldwide 2017-2028, May 5 2023 <https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/#:~:text=The%20global%20estimated%20cost%20in,to%2013.82%20trillion%20U.S.%20dollars> accessed 16 May 2023

1990 enacted to stem the flow of cases like *R v Gold & Schifreen*[12] from becoming the norm. In Nigeria the Cybercrime Prohibition Prevention Act 2015(CPPA) was passed to tackle all forms of cyber-criminalities on the web. Equally law enforcement agents (LEAS) have been trained and equipped to tackle the global cybercrime menace, despite all these efforts cybercrime is on the increase. Emphasis in curbing cyber insecurity focuses on technological and legislative aspects with less emphasis on hacker conversion strategy.[13] We argue in this article that the traditional means of curbing crime has failed woefully as evidenced by the growing number of cybercrime and the fact that cybercrime is in a class of its own in terms of criminality. It's a technical, sophisticated crime requiring expertise skill and computer forensic experience. Given its danger to global economy and world peace, a radical manner of tackling this unprecedented crime is advocated and the time to do so is now.[14] This article is divided into four parts part II of this article following this introduction examines the concept of hacking drawing out the positives and negatives of hacking as a strategy to curb cyber criminality on the web. In part III we analyze the United Kingdom approach of using hackers to curb cybercrime and effectiveness of this measure. in part IV we proffer the challenges that cybercrime inflict on a growing economy like Nigeria and part V highlights on how adopting the United kingdom strategy could help greatly reduce if not eliminate cybercrime this is followed by concluding remarks.

2. The Concept of Hacking and Its Dangers

Historically, the current connotation of the word "hack" was coined at Massachusetts Institute of technology MIT in 1955.[15] The earliest

---

[12] (1988) AC 1060

[13] Samuel Chng, Han Yu Lu, Ayush Kumar, David Yau, Hacker types, motivations and strategies: A Comprehensive Framework [2022] (5) *Computers In Human Behavior* Reports) ,1

[14] V Griman, To Catch A Thief In The Cloud: Paradigm For Law Enforcement [2014], 13,(3) *Journal of Information Warfare*, 68-78

[15] The generic term of Hacking is used to describe unauthorized access to the internet including spread of viruses and malware, denial of service attacks Debra Hopper, History of Computer Hacking and Cybersecurity Threats: From the 50s to Today,

recorded computer hacking occurred in 1963.[16] Hacker beginnings are entrenched deeply in academia; Hacking is a complex field of activity.[17] According to Oliver De Jarvis and Adriane B Randolph "there is no clear definition of what a hacker is, or who may or may not be considered a hacker".[18] However attempts have been to conceptualize hacking. Hacking has been defined as the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data.[19] The idea of hacking may conjure images of electronic vandalism and espionage.[20] Hacking is not always a malicious activity, but the term has mostly negative connotations due to its association with cybercrime. A majority of hackers begin as novices before acquiring more skills, knowledge and experience to become professionals.[21]

Hackers in cyberspace are grouped into malignant cum black hat hackers and ethical/ penetration testing (PenTest) hackers. [22] Malignant Hackers are a group of cybercriminals who work with relative impunity, beyond traditional jurisdictions and physical borders.[23] They commit atrocities on the web by infiltrating a victim's device to steal passwords, credit card numbers, pilfer bank accounts,

---

April 21 2023 <https://securityboulevard.com/2023/04/history-of-computer-hacking-and-cybersecurity-threats-from-the-50s-to-today/> accessed 14 May 2023.

[16] ibid

[17] <https://courses.cs.washington.edu/courses/csep590a/06au/projects/hacking.pdf> accessed 14 May 2023

[18] Oliver DeJarvis and Adriane B Randolph ,Hacker Definitions In Information Systems Research [2022](62) (2) *Journal Of Computer Information Systems* 397

[19] What is hacking? And how to prevent it< https://www.kaspersky.com/resource-center/definitions/what-is-hacking> accessed 27 May 2023

[20] Jon Erickson, *Hacking,The Art Of Exploitation* (San Francisco: No Starch Press 2008)9

[21] J Beveren A Conceptual Model Of Hacker Development And Motivations) [2001] (1) (2) *Journal of E-Business*, 16

[22] Raymond, Eric S. 2003. The Art of Unix Programming. Harlow: Addison-Wesley

[23] Samuel Chng, Han Yu Lu, Ayush Kumar, David Yau, Hacker Types, Motivations And Strategies: A Comprehensive Framework, [2022] (5) *Computers In Human Behavior Reports*,1

and install malicious software. [24]These Hackers target potential victims via email and websites. Motivations for malignant hacking vary.[25]The biggest motivation is often financial gain.[26] Malignant Hackers make money by stealing passwords, accessing bank or credit card details, holding information to ransom, or selling victims data to other hackers or on the dark web.[27] A common tenet to all black hats that ties them together is that they knowingly commit mischief with the full intent of committing such acts.[28] In McKinnon *v. United States*,[29] a forty-two year old British man identified US Government network computers and gained unauthorised access to administrative accounts while surfing the web. Having gained access to those accounts, he installed unauthorised malware that enabled him to alter data on the computers. He was able to scan over 73,000 US Government computers and networks. The computers the appellant accessed were: 53 army computers, 26 navy computers, 16 National Aeronautics and Space Administration (NASA) computers among others.

He also deleted data from them including critical operating system files from nine computers, which shut down the entire US army's network of over 2000 computers for 24 hours, significantly disrupting governmental functions; 2,455 user accounts on a US army computer was compromised, causing these computers to reboot and become inoperable.

The havoc the appellant wrecked on the United States defence computers was massive. Besides genocide cybercrimes is one of the most heinous crimes that the world have witnessed, nothing exceeds

---

[24]Eric S Raymond,The Art of Unix Programming.(Harlow: Addison-Wesley 2003.)16

[25] J Van Beveren - A Conceptual Model of Hacker Development and Motivation [2000] **(1) (2)**Journal *of E-Business,* 2

[26] Lilan Ablon, The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data 15 March 2018 <https://www.rand.org/pubs/ testimonies/CT490.htm>l accessed 20 May 2023

[27] ibid

[28] Robert J. Sciglimpaglia, Jr. Computer Hacking: A Global Offense [1991] (3)(1) *Pace International Law Review* 201

[29] [2008] UKHL 59.

this crime in the wanton destruction of property except perhaps nuclear warfare. Besides causing massive damage to computer networks, hacking is the most sophisticated and newest form of rigging elections;[30] Two days before France's presidential runoff in May 2017, hackers dumped a 9GB of leaked emails from the party of left-leaning front-runner (now French president) Emmanuel Macron in a bid to manipulate the elections.[31] Nigeria was not spared this cyber assault; in the just concluded 2023 elections the Nigerian government announced that it recorded a total of 12.9 million (12,988,978) cyber attacks, originating from both within and outside Nigeria during the elections.[32] It's not uncommon these days to hear that a trove of voter data was breached or exposed somewhere in the world.[33]

Not all hacking is malicious like the McKinnon case. Ethical /penetration testing (PenTest) hackers are hackers who work with the intention of aiding the administrators of a network in strengthening their security measures.[34] Ethical hacking is the practice of testing a computer system, network or application to find security vulnerabilities that could be exploited by malicious hackers.[35] Ethical hackers assist in uncovering possible vulnerabilities on a computer or network. An ethical hacker penetrates system defenses and looks for any openings that may be taken advantage of by black hat hackers. Firms use this information to enhance system security in an effort to

---

[30] Obinne Obiefuna-Oguejiofor, Advancing Electronic Voting System In Nigeria's Electoral Process: Legal Challenges And Future Directions. [2018] (9) (2) *The Journal Of Sustainable Development Law And Policy* 287-213

[31] Lily Hay. Newham, "The Biggest Cyber Security Disasters Of 2017"<https://www.wired.combiggest-hacks-so-far/> 1 July 2017accessed 14th February 2023.

[32] Mary Izuaka Nigeria recorded 12.9 million Cyber attacks during presidential, NASS elections – Minister 15 March 2023https://www.premiumtimesng.com/business/business-news/587712-nigeria-recorded-12-9-million-cyber-attacks-during-presidential-nass-elections-minister.html accessed 21 May 2023

[33]ibid

[34] Brian Alleyne, Computer Hacking As A Social Problem in Javier Trevino (eds), Cambridge handbook Of Social Problems (Cambridge: Cambridge University Press 2018) 127

[35] ibid

lessen or stop any prospective threats.[36] Ethical hackers use the same tools and techniques as malicious hackers, but they do so with permission from the owner of the system being tested.[37] For Jeff Schmidt, Head of Business Security and Governance at British Telecommunications, "Today's networks are a myriad of system applications. Change in technology, compression of the IT workforce, and pressure to expand network presence add up cyber risk for companies. Having good white hat hackers on staff can be an effective countermeasure against malicious hackers."

Besides grouping hackers into malignant and ethical hackers, Samuel Chng et al, grouped hackers based on the table below[38]

Novices	Re-use codes/scripts/malware found from Internet. Not careful enough to cover their online tracks.
Cyberpunks	May use existing codes/scripts but with some modifications or write their own ones. Attack vectors include bricking to cause damage to victim systems, carry out Denial of Service attacks. Focused on garnering public and media attention.
Insiders	Use internal confidential knowledge of a company's cyber-infrastructure to launch attacks. May transfer sensitive

[36] Yash Naraynbhai Patel , Dr. Darshanaben Dipakkumar Pandya , Dr. Abhijeetsinh Jadeja, An Influence of Ethical Hacking in Civilization, [2023] (10) (1) *International Journal of Scientific Research in Science and Technology* 195

[37]Prabhat Kumar Sahu, Biswamohan Acharya, A Review Paper On Ethical Hacking [2020] (11) (12) *International Journal of Advanced Research in Engineering and Technology* 163

[38]Samuel Chng, Han Yu Lu, Ayush Kumar, David Yau, Hacker Types, Motivations And Strategies: A Comprehensive Framework, [2022](5), *Computers In Human Behavior Reports*1

	organizational data to their own devices, access company databases/servers, cloud storage etc
Old Guards	Use customized codes to reveal vulnerabilities in existing systems. Track malicious hackers using cyber forensic techniques. Includes white hats and grey hats.
Professionals	Perform sophisticated attacks using the full repertoire of attack vectors and customized code. Careful to not leave any online trail behind
Hacktivists	Employ attack vectors such as SQL injection, web server to take over databases and leak their contents, deface high-profile websites, etc
Crime Facilitators	May offer cybercrime as a service to criminals by helping them carry out phishing campaigns etc
Crowdsourcers	Join forces and pool their skills together for tasks such as developing new malware etc.
Petty Thieves	Use attack vectors such as ransomware to gain credit card or bank account details
Digital Pirates, Online Sex Offenders	Steal copyrighted content directly or indirectly and leak them. Befriend potentially vulnerable victims on Facebook or other social media.

3. The Use of Hackers to Curb Cybercrime: The United Kingdom Approach

The practice of ethical hacking has recently been the focus of much debate among computer security professionals. Nations are adopting ethical hacking into their cybercrime eradication strategy. One such

nation is the United Kingdom. The use of hackers to curb cybercrime in the United Kingdom criminal justice system is gradually being accepted. The UK applies the ethical hacker strategy in eradication of cybercrime through three main modes namely via consultancy/partnership, permanent employment, ethical hacker friendly policies and education. The 2017 Ransomware incident illustrates the consultancy / partnership mode of eradicating cybercrime in conjunction with ethical hackers. The United Kingdom partnered with a hacker Marcus Hutchins to stop the spread of WannaCry virus harming the health services in the UK. WannaCry a ransomware found its way into major computer system networks, spreading like wildfire crippling businesses.[39] This was the first time in a decade a computer worm attacked computers on a massive scale. The UK.'s National Health Service (NHS) was one of the biggest organizations hit, forcing doctors to turn patients away and emergency rooms to close. The then British Prime Minister Theresa May called it an "International cyber-attack," one the United Kingdom government seemed powerless to stop. A British hacker Marcus Hutchins, was drafted to help shut down the WannaCry cyber attack. Hutchins, along with the UK's National Cyber Security Centre, worked tirelessly to contain the virus. He successfully found a "kill switch" that slowed the effects of the WannaCry virus.[40]

The UKs Ministry of Defence MoD has also incorporated this consultancy/partnership policy; The Ministry of Defence became the first government department to pay ethical hackers to thwart cyber criminals. Ethical hackers were drafted to work with the MoD cyber teams in order to ensure better security across defence networks and its 750,000 devices.[41] Christine Maxwell, the MoD's chief information

[39] Besides the United Kingdom WannaCry affected other 300,000 computers in 150 countries. Telecoms giant Telefonica was also hit, as well as shipping giant FedEx, car maker Renault, Germany's rail system and several Russian government departments were also affected by this malware.

[40]<https://techcrunch.com/2019/07/08/the-wannacry-sinkhole/> accessed 22 May 2023

[41] Charles Hymas, Cyber-detectives could get new powers to infiltrate hacking and scamming gangs 11 May 2021 <https://www.telegraph.co.

security officer, state "Working with the ethical hacking community allows us to build our tech talent and bring more diverse perspectives to protect and defend our assets: despite it being a non-traditional approach for the MoD, it is common practice among the technology industry and has already been adopted by the US Department of Defence. It is an essential step in reducing cyber risk and improving resilience." In a first for the MoD, 26 ethical hackers were drafted into 30-day challenge aimed to identify and fix vulnerabilities in cyber systems to strengthen MoD Computer Defense's security and to ensure better resilience.[42] Giving his opinion about MoD's partnering with ethical hackers, CEO Hacker one Marten Nickos opined "Governments worldwide are waking up to the fact that they can't secure their immense digital environments with traditional security tools anymore. Having a formalized process to accept vulnerabilities from third parties is widely considered best practice globally, with the U.S government making it mandatory for their federal civilian agencies this year. The U.K MoD is leading the way in the U.K government with forward-thinking and collaborative solutions to securing its digital assets and I predict we will see more government agencies follow its example." [43]

Equally the UK has in place policies that encourage the use of hackers to protect computer systems.[44] The government taking steps to further reduce the levels of cyber security risk in its supply chain introduced the Cyber Essentials scheme.[45] Businesses are required to provide evidence that they have undergone a successful Cyber Essentials evaluation. The evaluation expects partner' systems to have in place

---

uk/news/2021/05/11/cyber-detectives-could-get-new-powers-infiltrate-hacking-scamming/> accessed 22 May 2023

[42] Ethical hackers collaborate with Defence to strengthen cyber security 3 august 2021 <https://www.gov.uk/government/news/ethical-hackers-collaborate-with-defence-to-strengthen-cyber-security> accessed 22 May 2023

[43]ibid

[44] The University of Abertay in Scotland United kingdom, was licensed by the UK government to offer ethical hacking at bachelor and masters level

[45] < https://www.cyberessentials.ncsc.gov.uk/].> accessed 22 May 2023

security controls that meet the requirements of Cyber Essentials Plus.[46]Furthermore businesses bidding for central government contracts which involve handling sensitive and personal information are required to obtain Cyber Essentials Certification to qualify for the bid.[47] To satisfy these requirements business hire ethical hackers to sniff out vulnerabilities in computer systems.

Employment wise, the UK government offers permanent employment in various government departments. This is regularly advertised in her national dailies. [48] The ethical hacker becomes a staff of the government. His or her function is to infiltrate computer systems of the government through attacks. The UK Cabinet Office offers an annual salary of up to £60,000 in a bid to recruit an in-house ethical hacker.[49] In a recent development, hackers working for the UK's National Cyber Force (NCF) made hundreds of thousands of stolen credit cards worthless to criminals, according to the head of GCHQ, Sir Jeremy Fleming. He opined, "The operation meant tens of millions of pounds in potential fraud against the British economy were avoided".[50]

The UK is at the vanguard of using education to curb cyber criminality. The University of Abertay in Scotland United Kingdom was licensed by the UK government to offer ethical hacking as a course at bachelor and masters degree level. Launched in 2006, University of Abertay's Ethical Hacking degree was the first of its kind in the world.[51] Years later University of Coventry equally in the United Kingdom followed suit. Ethical hacking and cybersecurity as a

[46]ibid
[47] ibid
[48] Sam Trendall, cabinet officer offers 60 k for in-house ethical hacker 15 September 2021 <https://www.publictechnology.net/articles/news/cabinet-office-offers-%C2%A360k-house-ethical-hacker> accessed 22 May 2023
[49] ibid
[50] Alexander Martin**,** UK government hackers destroyed hundreds of thousands of stolen credit card details held by criminals< https://news.sky.com/story/uk-government-hackers-destroyed-hundreds-of-thousands-of-stolen-credit-card-details-held-by-criminals-12609745> accessed 22 May 2023
[51]< https://digital.ucas.com/coursedisplay/courses/f6638327-c9d6-b294-8a9c-bf7c7d06fb59?academicYearId=2023> accessed February 5 2023

course is equally offered in this university at masters and undergraduate level.[52] The students obtaining ethical hacking degree are expected to learn a deep understanding of cybercrime so they can master the skills to stop hackers;[53] they are taught to identify who hackers typically are, the techniques they use to break into systems and the way to defend against them.[54] They also learn how to examine computers and networks for digital vulnerabilities, how to fix them. Equally they are taught a practical and offensive approach of cybersecurity, by deliberately breaking computer systems and building cybersecurity defenses. The course combines computer networking, digital forensics and expert development as well as programming.

4. Cybercrime: Nigeria's Albatross

Cybercrime is a scourge to Nigerian youths as a good number of them are involved in this crime.[55] Nigeria is the cybercrime capital of Africa. Nigerian internet fraudsters become more proficient at scams over the years, employing more sophisticated tactics to carry out these scams. Of Nigeria's 214million population, 109million have access to the internet which affords cyber-deviants an opportunity for crime.[56] The digital revolution of e-banking has resulted to an increase in internet fraud. The rising rate of the internet fraud is also traceable to increasing access to digital literacy, near pervasive internet availability and access to smart devices.[57]

---

[52]< https://www.coventry.ac.uk/course-structure/ug/eec/ethical-hacking-and-cyber security-bsc/>

[53] ibid

[54] ibid

[55] Sharon Lin the long shadow of Nigerian Prince Scam https://www.wired.com/story/nigeria-cybersecurity-crime-antiblackness/18 April 2022 accessed February 5 2023

[56] Simon Kemp, Digital Nigeria 2022 15 February 2022 < https://datareportal.com/reports/digital-2022-nigeria> accessed February 5 2023

[57] Gabriel Ogunjobi, Internet Fraud Is Destroying Nigeria Thanks To The Government 23 September 2019 <https://www.africanliberty.org/ 2019/09/23/internet-fraud-is-a-problem-in-nigeria-but-the-government-is-worse/>

In 2021 Salau Femi hacked into the System of a First-Generation Bank and made away with One Billion, Eight Hundred million Naira.[58] The Economic and Financial Crimes Commission (EFCC), has said more than 70 per cent of Nigerian youth might soon become ex-convicts if the present high rate of their involvement in cybercrime was not stopped.[59]Cybercrime is so entrenched among Nigerian youths that in 24 hours 33 cybercrime conviction were recorded in Benin.[60]

Foreign direct investment is hampered by the lack of confidence in Nigerian cyberspace.[61] Director General National Information Technology Development Agency (NITDA) Kashifu Inuwa, stated that the goodwill of Nigeria in the international stage is eroded as a result of cybercrime.[62] Africa Cyber Security Report states that various corporate entities in Nigeria and individuals collectively lost a total sum of $800 million to cyber attacks in 2018.[63] Despite the promulgation of the CPPA 2015 cybercrime is on the increase in Nigeria instead of decreasing. In United States Of America V Obinwanne Okeke,[64] Okeke a Nigerian was convicted and sentenced to 10 years in prison for his involvement in a computer-based intrusion fraud scheme that caused approximately $11 million in known losses to his victims. Okeke entered into a plea bargain agreement with the U.S. authorities and pleaded guilty. This case and a host of other cases contribute to lack of trust and confidence in the Nigerian cyberspace. These scams have continued to have negative effects on the image of Nigerians across the globe, as they are always perceived as fraudsters.

---

[58] <https://www.specialfraudunit.org.ng/en/?p=1186> accessed February 5 2023

[59] 70 % of Nigerian Youths May Soon Become Ex Convicts Says EFCC <https://www.thisdaylive.com/index.php/2021/08/27/70-of-nigerian-youths-may-soon-become-ex-convicts-says-efcc/> accessed 5 February 2023

[60] Daily Trust, EFCC Records 33 internet fraud Convictions In 24hours In Port Harcourt 27 August 2021 <https://dailytrust.com/efcc-records-33-internet-fraud-convictions-in-24-hours-in-port-harcourt/> accessed 5 February 2023

[61] Ife Ogunfa, Cybercrime Eroding Business Reputation – NITDA Punch Newspapers (Lagos, 8 October 2019) 19

[62] Ibid

[63] Omobayo Azeez, <https://www.businessamlive.com/cyber-crime-cost-nigeria-n288bn-in-2018/> accessed 5 February 2023

[64] Unreported Case 4:19-Cr-00084-RBS-RJK

This reputational challenges Nigeria face contributes to ill treatment of her citizens abroad.[65] They have also affected international recognition of the country's young entrepreneurs, and the granting of visas to those with legitimate business interests in other parts of the world.[66]

Nigeria loses about N127 billion yearly to internet fraud, an amount which represents 0.08% `of Nigeria's gross domestic product, a report has revealed.[67] The report also shows that the global yearly cost of cybercrime reached $6 trillion at the end of 2021.[68] In five years alone a particular new generation bank lost N871m to scammers and hackers.[69] The Nigeria Inter-Bank Settlement System (NIBSS) reported that the first nine months in 2020, Nigerian banks lost over N5bn to fraud related to electronic transfers.[70]

Not content with just internet fraud, two new trends have been adopted by Nigerian cybercriminals to maximize the havoc they wreck on the web.[71] The first trend is the Yahoo- Yahoo Pro Max or Yahoo Plus. Yahoo- Yahoo Pro Max entails a mix of murder and scam. Nigerian internet fraudsters are now engaging in a lethal combination of ritualistic murder and internet fraud in a bid to get rich quicker. Barbarism and depravity is the culture for this trend. The rise of the Yahoo-Yahoo Promax stemmed from victim awareness of cybercrime. As more people became alert about internet scams, it is becoming

---

[65] David Hundeyin, Opinion FBI Fraud Busts dent Nigeria's Global Reputation August 29 2019 <https://edition.cnn.com/2019/08/29/africa/nigeria-fbi-fraud-bust-intl/index.html> accessed February 5 2023

[66] Abdullateef Aliyu and others Nigerians Explore Egypt, Morocco, Others After Dubai Visa Ban 31 December 2022 <https://dailytrust.com/nigerians-explore-egypt->morocco-others-after-dubai-visa-ban/ accessed February 5 2023

[67] Omon Okhuevbie Nigeria Loses 127bn To Internet Fraud Annually – Reports 13 may 2021 https://independent.ng/nigeria-loses-127-billion-to-internet-fraud-annually-reports/ accessed 27 May 2023

[68] Ibid

[69] Ibid

[70] Ibid

[71] Yahoo plus Nigerian youths ritual killings and the quest for wealth <https://www.thisdaylive.com/index.php/2022/03/14/yahoo-plus-nigerian-youths-ritual-killings-and-quest-for-wealth/> accessed 27 May 2023

increasingly tough to get victims to part with money. Young Nigerians boys started engaging native doctors to make charms for them to succeed in defrauding their victims. The native doctors in turn ask for human body parts for sacrifice. In May 2023, a 29-year-old internet fraudster identified as Amos Olaleye, was arrested by the Lagos State Criminal Investigation Department SCID on a stop-and-search duty on Itamaga-Ikorodu Road while on his way to throw his sister's corpse into a river. He informed the Nigeria Police how he in connivance with his mother killed his sister. In his confessional statement, he also admitted having sexual intercourse with his deceased sister after killing her. The suspect alleged that he was instructed to dump the corpse in a river after her vital organs had been removed. He explained, "My mother was the one who took me to a native doctor who stated I would have to murder my most loved siblings if I wanted to be successful. I am into Yahoo business. It took me months before I could make up my mind if I actually wanted to embark on the killing. My mother kept encouraging me to kill my sister so that we could bring an end to the poverty in the family. My mother planned the entire incident by going out to buy poison which she put in my sister's food. The native doctor also instructed that I must sleep with my sister's corpse and suck her vagina before throwing the corpse into a river for the ritual to be completed.[72]

The second trend which points to the proliferation of cybercrime in Nigeria is the establishment of cybercrime "academies" where young cybercriminals are taught the rope for internet fraud by mentors.[73] More than fifty cybercrime "academies" have been identified over the course of nine months.[74] The training academies are springing up to initiate new members to join the cybercrime cult. The Economic and Financial Crimes Commission (EFCC) recently arrested the owner of a

[72] Eugene Agha, How Our Mum Forced Me To Kill My Sister For Ritual 10 May 2023 https://dailytrust.com/how-our-mum-forced-me-to-kill-my-sister-for-ritual/ accessed 27 May 2023

[73] EFCC arrests proprietor of yahoo yahoo school in Benin December 16 2022< https://www.thecable.ng/efcc-arrests-proprietor-students-of-yahoo-yahoo-school-in-benin> accessed 25 February 2023

[74] Ibid

"yahoo yahoo" academy through a sting operation in Abuja; [75]the Abuja arrest was similar to an earlier one in Eket, Akwa Ibom State where 23 suspects including operators and trainees were nabbed by officials of the EFCC. The suspects were between the ages of 19 and 35 years.[76] They were undergoing training in various aspects of the internet scams such as love scam, online trading scam, theft identity, among others From the various arrests and convictions made by the EFCC so far, it shows that cybercrime in Nigeria is is nowhere near extinction. It is rather growing in leap and bounds. If anything at all, it is on the rise. Young men and women are still plunging into the business of cybercrime. There are strong indications that the crime will continue to blossom.

5. Tackling the Nigerian Cybercrime Situation: Lessons from the United Kingdom.

As seen in the preceding section of this article. Cybercrime is an epidemic among Nigerian youths. It is costing the country economic and social goodwill. Use of ethical hackers as agents of cyber deterrence has favored the United Kingdom, in making her cyberspace safe from cybercriminals. The UK applied the employment model, the education model and the consultancy model of cyber deterrence. These models of cybercrime deterrence have been largely successful. Given the massive failure of her cyber-deterrence policy as evidenced by the increasing numbers of cybercriminal among her youth, it behooves Nigeria to transplant the UK model in her bid to crime-proof her cyberspace. Educationally as can be seen in the UK universities offering ethical hacking as undergraduate and post graduate course; Nigerian government should adopt this policy by licensing government and private universities to offer this essential course. Nigeria has a large percentage of youth population that are being trained in higher

---

[75] Ishola oludare, yahoo, yahoo training school discovered in Abuja 18 February 2021 <https://dailypost.ng/2021/02/18/yahoo-yahoo-training-school-discovered-in-abuja/> accessed 25 February 2023

[76] Felix Emeakpore Eboibi, Omozue Moses Ogorugba, Cybercrime Regulation And Nigerian Youths Increasing Involvement In Internet Fraud: Attacking The Roots Rather Than The Symptoms [2023] *(26)(S2), Journal of Legal, Ethical and Regulatory Issues*, 1-17.

institutions and there is need to give them the right training with the right curriculum to enable them come up with innovative digital solutions that could discourage them from engaging in social vices like cybercrime.[77] With the springing up of cyber fraud academies around the country, it is damning that Nigerian citizens prefer to establish cyber fraud academies when legitimate Information Technology/ Ethical hacking institutions could have been established. This is sheer misapplication of entrepreneurial drive.[78] Converting these cyber-fraud academies into a licensed course is thus advocated. The job is made easier for Nigerian government as there is already an established platform i.e. the academies. The students and the instructors should be spared jail and become the pioneer students and lecturers of the course. The ethical hacking course should be open also to the members of the public. Adopting this cyber deterrence model benefits both the government and citizens.

In examining the employment / consultancy model to interrogate its fitness for purpose for cybercrime eradication, employing Nigerian hackers to help prevent cybercrime is beneficial for both the government and the cybercriminals. The psychological boost of payment of salary will secure long term loyalty. Enrolling hackers on a payroll also solves the problem of unemployment that Nigeria is facing. Cybercriminals involved in solving cybercrimes and paid as staff of the EFCC, police etc reduces the number of out of job youths. For one of the major attractions of cybercrime is the fact that youths are unemployed.[79] Once employed, Cyber criminals will highlight the weak points in cyber security infrastructure and instruct the law enforcement agents on digital forensic skills and as they infiltrate networks and computer system to catch cybercriminals. Where one is able to create a virus, or hack into a government computer networks, one can equally create a program to stop hacking and malware. The private sector will benefit from the expertise of these cybercriminals

---

[77] Sonny Aragba-Akpore <https://www.thisdaylive.com/index.php/2022/06/01/digital-literacy-and-rising-cyber-crimes> accessed 27 May 2023

[78] Ibid

[79] Anah Bijik Hassan, D L Funmi, Julius Makinde, Cybercrime in Nigeria: Causes, Effects and the Way Out [2012] (7) (2) *Journal of Science and Technology* 62

that have been converted to help contain cybercrime. Their assistance in spotting weaknesses, unearthing vulnerabilities in applications in servers of these businesses saves tremendous amount of finances for these companies. Hiring of these hackers has numerous advantages besides solving crimes. Firstly it tackles the unemployment challenges Nigeria is facing. Nigeria has been dubbed the poverty capital of the world, the number of Nigerian youth unemployed is alarmingly high[80] engaging them in meaningful employment reduces the rate of cyber criminality. Secondly the government obtains income by the taxing the salaries of these now converted ethical hackers. For the hackers, from an economic perspective, gainful employment and a legitimate paycheck is more rewarding than living in fear of law enforcement officers because of their criminal activities on the web. They equally are rehabilitated because being employed legitimately by government or the private sector offers them a consistent and steady stream of income and a chance of climbing the career ladder.[81]Unlike paid employment, Cybercriminals like hackers don't get finances all the time as their victims don't get conned frequently. Regular salary makes them plan effectively, save money and explore their potentials.[82]

Equally the current issue between the federal government and the state government concerning feeding prisoners will be partially solved where instead of incarceration these cybercriminals are put to pasture to help detect and solve cybercrime.[83]

Engaging in crime has destructive negative traits namely shame, guilt, fear, lack of identity, lack of status and sense of purpose. Where one is

---

[80] Kingsley Nwezeh, Hameed Shittu, 70% Of Nigerian Youths May Soon Become Ex-Convicts, Says EFCC <https://www.thisdaylive.com/index.php/2021/08/27/70-of-nigerian-youths-may-soon-become-ex-convicts-says-efcc/> accessed 3 May 2023

[81] Matthew Modini and others, Mental health benefits of employment: Results Of A Systematic Meta-Review[2016] (24) (4) *Australasian Psychiatry* 332

[82] ***Obed Uchenna Chukwuka*** Internet Fraud: The Menace of 'Yahoo Boys' And The Deceitfulness Of Riches [2022] (5)(2)*SGOJAHDS Journal* 87

[83] Christiana Nwaogu Federal Govt To Stop Feeding Of Prison Inmates <https://leadership.ng/federal-govt-to-stop-feeding-of-prison-inmates/> accessed 3 May 2023

gainfully employed in a legitimate setting; it instills a whole array of positive traits, including good work ethic, capacity to take responsibility, opportunities to express creativity, skills without fear of Law enforcement agencies.[84] Equally being in full time legitimate employment confers psychological benefits such as social inclusion, enhanced self-esteem, integration, social skills and confidence. This hacker conversion strategy is a win-win situation in all ramifications. With a large percentage of youth population in Nigeria, the country needs to tap into this God given gift and position these youths to use their digital skills positively.

6. Conclusion

It takes a misfit to catch a misfit; it takes a deviant to catch a deviant. The hiring of hackers to crack cybercrime though unconventional is essential. Cybercrime is unprecedented, technical, sophisticated and involves a lot of forensics. The hackers understand the dynamics of cybercrime. Conservative measures to curb cybercrime are no longer effective. Working with hackers will encourage transfer of skills to the law enforcement agencies as they will learn the forensics skills of cybercrime at the feet of the masters of this crime. Nigeria should embrace this model as the benefits far outweigh the disadvantages. The age old mentality that criminals should be punished and incarcerated which makes the hacker conversion theory unpalatable to some stakeholders should be interrogated. The benefits of crime solving, crime bursting, employment opportunities and educating our youths which the cybercrime eradication model confers should not be sacrificed on the altar of punishment of crime.

[84] S Phillips, K l Sandstrom - Parental Attitudes Toward Youth Work [1990] (22) (2) *Youth & Society*, 160–183.