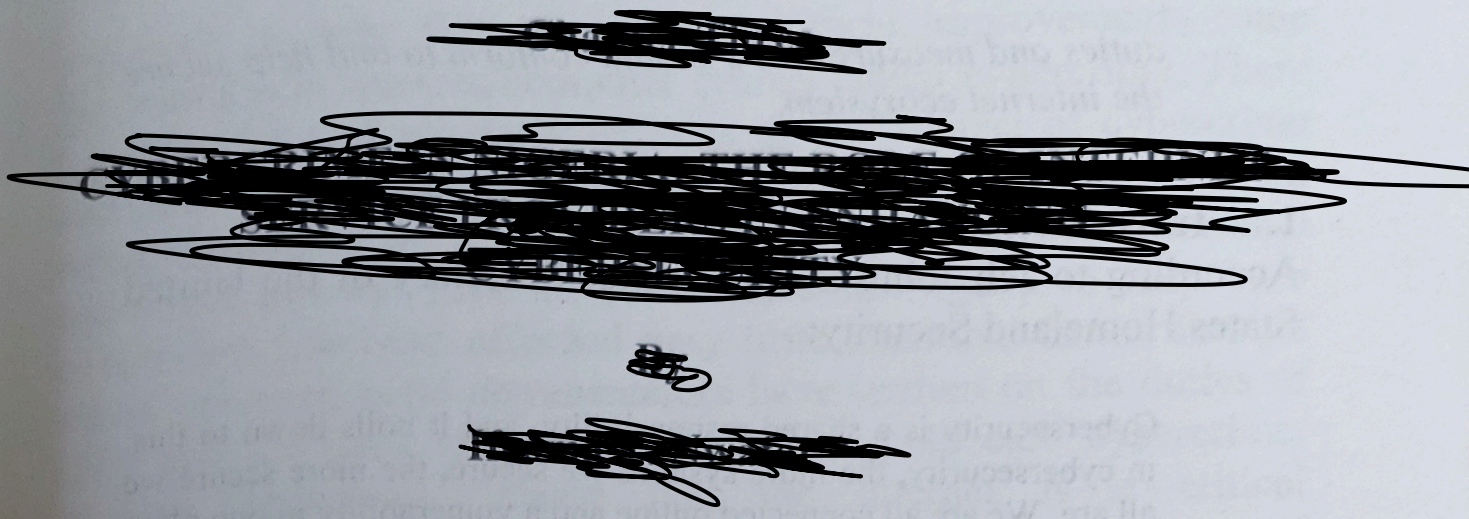
CYBERCRIME AND THE LAW

ISSUES AND DEVELOPMENTS IN NIGERIA

IFEOMA E. NWAFOR



Abstract

Internet connectivity has shortened time and space. It has enhanced the transfer of information and provided unlimited opportunities for commercial, educational, communication, social and individual activities. These electronic and globalized benefit is accompanied with an increase in cybercrime activities. Nigeria is ranked highly in global internet crimes and in consequence, economic growth has plummeted, and international investors' confidence is rock bottom. Data breaches fundamentally, affects consumers' confidence in the cyberspace. Internet Service Providers (ISPs) have a crucial role to enhance cyber security and boost internet users' trust in the internet ecosystem. This article examined the ISPs role in promoting cyber security. It found that ISPs are not doing enough to police or secure the cyberspace. The objective of this paper is to offer insights on the copious opportunities ISPs can furnish to cyber security enhancement based on the edge and bearing they possess in the cyberspace. ISPs can offer more than the compliance-checkbox; it should provide continuous protection for consumers. This article adopts the doctrinal method of legal research. It analyses the Cybercrime Act 2015. It found that there are gaps with respect to the duties of ISPs and in the area of enforcement. It canvasses for an amendment of the Act to specifically provide the strategic

Published by

Kraft Books Limited

6A Polytechnic Road, Sango, Ibadan
Box 22084, University of Ibadan Post Office
Ibadan, Oyo State, Nigeria
© +234 (0)803 348 2474, +234 (0)805 129 1191
+234 (0)803 350 9421, +234 (0)905 723 9357
E-mail: kraftbooks@yahoo.com;
kraftbookslimited@gmail.com

First published, 2022
by

CLDS Publishing 5b Lawani Oduloye Street, Oniru P O Box 73002, Victoria Island, Lagos, Nigeria.
Tel. +234 1 7039672614
Email: info@cldspublishing.com; info@clds-ng.com
Website: www.cldspublishing.com

This edition, May 2022

ISBN 978–978–918–759–1

DEDICATION

In loving memory of my mother, late Mrs Patience Nkem Nnamoko (forever in our hearts).

ACKNOWLEDGMENTS

I am eternally grateful to God Almighty, the author and finisher of my faith, for the gift of life and the successful completion of this book.

I have always wanted to publish a book on cyber laws in Nigeria, which was achieved through outstanding individuals' comments and insights. This book was developed from my doctoral thesis entitled "Cybercrime-Related Laws and Policies in Nigeria", completed in 2019 at the Faculty of Law, University of Nigeria. I am deeply grateful to my then supervisor, Professor Ifeoma P. Enemo, mni, for her diligence, guidance, and contributions to my thesis' success. I am also grateful to Professor Amucheazi, SAN and Dr E.U. Onyeabor, who watered my simple idea to write on cyber laws in Nigeria, which has evolved into a far better final product through their comments and encouragements on research.

I owe a debt of gratitude to Justice C.C. Nweze, Ph. D., JSC, for writing the Foreword and his insights on the subject. Much appreciation goes to Mr Abdul- Hakeem Ajijola (AhA) for kindly agreeing to write the advance book review and his comments which exude expertise in the field. I received valuable feedback on my ideas from Dr Chijioke Ifeoma Okorie. Thank you for your readiness to discuss concepts to improve this book. I am thankful to Dr M.E Ajogwu, SAN (my father in the legal profession) for his fatherly guidance and encouragement.

I wish to thank the Godfrey Okoye University community, particularly the Vice- Chancellor, Rev. Fr. Professor Christian Anieke, the Dean, Faculty of Law, Professor Gozie S Ogbodo, Professor Edwin Nwogugu, Professor B.O. Okere and my colleagues at the Faculty of Law. My gratitude goes to Professor C.N Okeke, Professor Edith Nwosu, Dr Samuel Nwatu, Rev. Fr. Professor Edwin Ezike and Dr Ndubuisi Nwafor for their research encouragement.

I am indebted to Professor Fabian Ajogwu, SAN, for his encouragement, support and for being a great role model. Mrs Dorothy Udeme Ufot, SAN, thank you so very much for being an immeasurable mentor all these years. I am grateful to the excellent Commercial Law Development Services editorial team, particularly Uche Ajogwu, Asuefai Ezekiel-Harcourt and Mrs Chioma Mordi, for their diligence and unwavering commitment to publishing this book.

I am eternally grateful to my dad, Engr. John Nnamoko, who always encouraged me to be the best version of myself. My sister Mrs Ngozi Nnaji and my brother, for their prayers and support. Finally, I could not have written this book without the love and incredible support of my awesome husband, Anayo and my babies, Serena, Ella, Sonia, Mark and Jason, for their love and patience with mummy.

Dr Ifeoma E. Nwafor

CONTENTS

CHAPTER 1

INTRODUCTION TO CYBERCRIME

1.1 INTRODUCTION

The internet, which is, inmany ways, the driving force of globalisation, helps to achieve global integration in all facets of life. The pace of development in recent years is unprecedented. However, it is commonplace to read in headlines of major cybersecurity breaches, whether at a corporation, government agency, or communication system. In Nigeria, there is a rapid increase in the number of internet users daily. As reported by the Nigerian Communications Commission (NCC), the number of internet users in Nigeria's telecommunications networks increased to 91.6 million in June 2017.[1] As the use of the internet heightens tremendously in Nigeria, so has the use and popularity of social media platforms.[2] Based on the Facebook report, Nigeria has one of the Continent's highest

---

1 Nigeria's Internet Rise to 91.6m' [2017] issue 22 (3) The Communicator <https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=1572:nigeria-s-internet-users-rise-to-91-6m&catid=32&Itemid=179> last accessed 4 October 2021.

2 Yomi Kazeem, 'More People use Facebook in Nigeria than anywhere else in Africa' [06 February 2016] <https://qz.com/611516/more-people-use-facebook-in-nigeria-than-anywhere-else-in-africa/> last accessed 5 October 2021. J Clement, 'Nigeria: Number of Internet Users 2017-2023' [9 August 2019] <https://www.statista.com/statistics/183849/internet-users-nigeria/> last accessed 5 October 2021.

smartphone penetration rates. It believes this number will escalate as smartphone subscriptions are expected to reach 95 million by 2019.[3] With the increase of internet users and the interconnectivity comes the rise in cybercrime. The survey conducted by the Centre for Strategic and International Studies (CSIS) on the estimated daily cybercrime activity is noteworthy. The review stated that:

> Cybercrime operates at scale. The amount of malicious activity on the internet is staggering. One major internet service provider (ISP) reports that it sees 80 billion malicious scams a day, the result of automated efforts by cybercriminals to identify vulnerable targets. Many researchers track the quantity of new malware released, with estimates ranging from 300,000 to a million viruses and other malicious software products created every day[4]

Furthermore, the Anti-Phishing Working Group (APWG) conveyed that more than 1.2 million phishing[5] attacks were recorded in 2016, with many linked to ransomware. The Privacy Rights Clearing House estimates that there were 4.8 billion records lost due to data breaches in 2016, with hacking responsible for about 60% of these breaches.

The recent information in the cyber-news is that Nigeria ranks 3rd in global internet crimes behind the UK and the United States. The Nigerian Deposit Insurance Corporate (NDIC) elucidated that fraud on the e-payment platform of Nigeria banking sector increased by 183 per cent between 2013 and 2014.[6] Also, the 2014 report by the CSIS, United Kingdom (UK), estimated the annual loss to cybercrime in Nigeria at about 0.08 per cent of the country's Gross

---

3 In 2018, Nigeria had 92.3 million internet users. This figure is estimated to increase to 187.8 million internet users in 2023.

4 Ibid.

5 Phishing is a type of social engineering attack which is fraudulent and often used to steal user data, including login credentials and credit card details.

6 Cyber-security: Nigeria Loses over N127bn Annually through Cybercrime' [2016] <*http://www.thisdaylive.com*>last accessed 26 September 2021.

Domestic Products. This figure represents about N127 billion.[7] Going by the estimates from the CSIS, cybercrime costs the global economy over US$400 billion annually.[8] The recent report by CSIS and McAfee[9] on cybercrime's economic impact estimated that cybercrime costs the world's economy almost $600 billion, or 0.8% of global GDP.[10] Cybersecurity Ventures envisages that cybercrime will cost the world $11.4 million every minute in 2021.[11] It estimates that cybercrime costs globally will increase by 15 per cent to reach $10.5 trillion annually by 2025.[12] Palo Alto Networks Incorporated stresses that Nigerian cybercriminals have graduated from traditional 419 email scams to more refined con games targeted at businesses than individuals.[13] Palo Alto's published paper on Nigeria offered a comprehensive assessment of financial losses incurred due to the criminal activities of Nigerian actors in cyberspace. It stated that:

> The losses inflicted by these actors have significant impacts on businesses worldwide. In 2015, an annual report released

---

7 'Nigeria Ranks 3rd in Global Internet Crimes' [August 2017] *<http://www.nigeriacommunicationsweek.com.ng>* last accessed 5 October 2021. Professor Umar Danbatta, Executive Chairman, NCC disclosed this during the 2017 Annual General Conference of the Nigerian Bar Association in Lagos.

8 Detlev Gabel, Bertrand Liard, Daren Orzechowski, 'Cyber risk: Why Cyber Security is Important' [July 2015] *<http://www.whitecase.com>* last accessed 29 September 2021.

9 MCAfee is an American global computer security software company that avers to be the world's largest dedicated security technology company.

10 James Lewis, 'Economic Impact of Cybercrime-No Slowing Down' [February 2018] CSIS *<https://csis-prod.s3.amazonaws.com>* last accessed 29 September 2021.

11 Steve Morgan, 'Cybercrime to Cost the World $10.5 Trillion Annually by 2025' [13 November 2020] <https://cybersecurityventures.com/cybercrime-will-cost-the-world-16-4-billion-a-day-in-2021/> last accessed 2 October 2021.

12 Ibid.

13 Peter Renals and Simon Conant, 'That Nigerian Prince Has Evolved his Game' [3 November 2016] *<http://researchcenter.paloaltonetworks.com>* last accessed 30 September 2021.

> by the FBI's[14] Internet Cyber Crime Centre identified 30,855 victims of traditional 419/overpayment scams resulting in losses in excess of $49 million. While that number is substantial, on 1st August 2016, Interpol announced the arrest of a Nigerian actor believed to be responsible for worldwide losses in excess of $60 million with over $15.4 million originating from one victim organisation.[15]

These surveys and estimates on monies lost to cybercrime and the increase of cybercrime in Nigeria and by Nigerians in the international scene are frightening. Cybercrime and security should be utmost priority for the Nigerian government. Nigeria has been described as a critical player in underground cyber activity and has become a destination for international cybercrime syndicates.[16] Also, Nigerian emails, the Advanced Fee Fraud or 419 frauds, is classified as one of the most common forms of fraud.[17] The Chairman, Senate Committee on Information and Communication Technology (ICT) and Cybercrimes, Senator Abdulfatai Buhari, stated that Nigeria is not ready for cyber-attacks.[18] He explained that Nigeria has the worst ICT culture than other nations, recording technology advances, particularly cybercrime. He believes that the lack of adequate ICT culture makes Nigeria inadequately equipped to tackle cyber-attacks. The ICT culture inadequacy shows that a lot has to be done in combating cybercrime in Nigeria. The global community already has a stereotypical conception of Nigeria. It is high time for the country to correct this impression that Nigeria is not a safe haven for

---

14 Federal Bureau of Investigation.

15 Renals and Conant, (n 13).

16 Noah Rayman, 'The World's Top 5 Cybercrime Hotspot' [2014] <*http://www.time.com*> last accessed 1 October 2021.

17 Peter Grabosky, *Cybercrime: Keynotes in Criminology and Criminal Justice Series* (New York: Oxford University Press 2016) 19.

18 Samson Atekojo Usman, 'Nigeria not Ready for Cyber Attacks- Buhari' <*http://dailypost.ng/2018/06/26/nigeria-not-ready-cyber-attacks-buhari/?utm_source=DailyPost+Newsletter&utm_campaign=6ac803bc54 Todays_headlines&utm_meduim=email&utm_term=0_7c25dc3ce6-6ac803bc54-227478289*>last accessed 5 October 2021.

cybercriminals. This can be achieved by creating an adequate law that accommodates the evolving nature of cybercrimes.

Cybercrime-related laws and policies regulating cybercrime in Nigeria are scattered over different legal instruments. These include the *Nigerian Criminal Code*,[19] *the Economic and Financial Crimes Commission (Establishment) Act*,[20] the *Independent Corrupt Practices and other Related Offences Act*,[21] the *Nigerian Communications Act*,[22] the *National Information Technology Development Act*,[23] *the Money Laundering (Prohibition) (Amendment) Act*[24] *and the Cybercrime Act*[25] amongst others. This book focused on these laws. Analysing these laws answers the question of overlapping laws investigating and prosecuting cyber- related offences and attendant issues. It identifies the gaps created by multiple legal orders in the fight against cybercrime. There are various consequences of conflicting provisions provided by numerous laws regulating cybercrime. The issue of which law would apply can arise. It can also serve as an escape route for a cybercriminal defendant in some cases.

1.2 THE BASIC CONCEPT OF CYBERCRIME

Cybercrime is challenging to conceptualise with exactitude. There is no universally accepted definition of cybercrime. The absence of conceptual and definitional clarity is problematic as it impacts the prevention and fights against cybercrime.[26] The term 'cybercrime' is used to describe computer-related crimes and crimes related to the internet. It has been defined by countries differently. The Australian

---

19 2004 LFN, Cap C 38.
20 2004, LFN.
21 2006.
22 2003.
23 2007.
24 2012.
25 2015.
26 Hamid Jahankhani, A Al-Nemrat, Amin Hosseinian-Far, 'Cyber Crime Classification and Characteristics' [November 2014] <*https://www.researchgate.net/lite.publication*>last accessed 12 September 2021.

government has defined it as computer offences under the *Commonwealth Code Act 1995*[27] involving unauthorised access to, modification, or impairment of electronic communications.[28] The United States has defined cybercrime as 'the use of cyberspace for criminal purposes as defined by national or international law'. In France, it is defined as 'acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime'.[29] Symantec Corporation defines cybercrime as 'any crime that is committed using a computer or network, or hardware device'.[30] Finklea and Theohary[31] believe that conceptualising cybercrime comprises several crucial elements and questions. These elements include: the location of criminal acts, whether the actors and victims are in the real and digital worlds, why these malicious activities are initiated, and who is involved in carrying out the acts?[32] The authors argue that borders and locations within the physical world are not replicated in the virtual realm. The keyboard, mouse, screen, and password are distinct boundaries that separate the physical and virtual domains. They argued further that there is a link between the digital world and the physical world without these different borders.[33] Fraudsters commit some crimes by physically collecting the skimming device or programming the device to broadcast the data to thieves over a network.

---

27 Commonwealth Code Act 1995, Part 10.7.

28 'Cyber Definitions' Nato Cooperative Cyber Defence Centre of Excellence <*http://ccdcoe.org/cyber-definitions.html*> last accessed 6 October 2021.

29 Ibid.

30 Symantee Corporation, 'What is Cybercrime?' <*http://us.norton.com/cybercrime-definition*>last accessed 30 September 2021.

31 Kristin Finklea and Catherine Theohary, 'Cybercrime: Conceptual Issues for Congress and U.S Law Enforcement' [15 January 2015] Congressional Research Service <*https://www.crs.gov*>last accessed 6 October 2021.

32 Ibid.

33 For example, the Point-of-Sale skimming.

Cybercrime has been described as a label of convenience as it refers to a wide range of crimes committed with the aid of digital technology.[34] It includes hacking, illegal interception of computer-mediated communications, illicit markets, theft of services, theft of data, theft of credit card details, espionage, piracy, fraud, sales, and investment fraud. Also, fraudulent ordering of goods, share market manipulation, Auction fraud, unauthorised funds transfer, embezzlement, ATM fraud, forgery, destroying or damaging data, website defacement, unauthorised public disclosures, interfering with the lawful use of a computer, malicious code, denial of service, spam, phishing, extortion, money laundering, offensive content, stalking and bullying, criminal conspiracies, cyberwar, and cyber-terrorism. Cybercrimes are crimes committed on the internet using the computer as either a tool or a targeted victim.[35]

In encapsulation, the term cybercrime and the scope of offences under the umbrella term are challenging to outline or conceptualise with precision. Many countries still have unclear perceptions of the meaning of cybercrime in their various legal instruments. This uncertainty arises due to multiple cyber-terminology variations, and new offences crop up daily in the internet ecosystem. It is submitted that a flexible/enveloping definition of cybercrime is essential so that new crimes committed in cyberspace can come within the ambit of such interpretation.

1.3 THE CONCEPT OF CYBERSECURITY

The concept of cybersecurity constitutes a great enigma to many countries and their law enforcement agencies due to the evolving nature of cybercrime and threat. There is no generally accepted definition of cybercrime. Choucri and others argue that there is no

---

[34] Peter Grabosky, (n 17).

[35] Computer Crime Research Centre, available on <*http://www.crime-research.org^Joseph06*> last accessed 19 September 2021.

agreed-upon understanding of the issue of cybersecurity.[36] There is no formal definition and no consensus on the spelling of the term cybersecurity. They highlighted the different spellings and meaning variations which are also problematic.[37] They stated that the inability to settle on a standard spelling and meaning amounts to divergence.

Cybersecurity is defined as 'the activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation.[38] It is described as 'the activity of protecting information and information systems (networks, computers, databases, data centres, and applications) with appropriate procedural and technological security measures'.[39] It has also been defined as 'the process of protecting information by preventing, detecting, and responding to attacks'.[40] Two definitions were developed during the 10th United Nations Congress on the Prevention of Crime and the

---

36 Nazli Choucri, Gihan Daw Elbait, Stuart Madnick, 'What is Cybersecurity? Explorations in Automated Knowledge Generation' [2012] *<http://www.ssrn.com/abstract=2178616>* last accessed 9 October 2021.

37 It has been spelt as cyber security, cyber-security and cybersecurity. This book adopts the spelling 'cybersecurity'.

38 'Explore Term: A Glossary of Common Cybersecurity Terminology' The National Institute for Cyber Security Careers and Studies, *<http://www.niccs.us-cert.gov>glossary>* last accessed 17 September 2021.

39 Atal M Tonge, Suraj S Kasture, Surbhi R Chaudhair, 'Cyber Security: Challenges for Society- Literature Review' [2013] *IOSR Journal of Computer Engineering* 12(2) *<http://iosrjournals.org/iosr-jce/papers/vol12/issue2/k01226775.pdf>* last accessed 9 August 2021.

40 Draft Strategy for Improving Critical Infrastructure Cyber security [2014] *http://www.natocooperativecyberdefencecenterofexcellence.com>* last accessed 17 August 2021.

Treatment of Offenders within a related workshop.[41] Cybercrime in the narrow sense (computer crime) covers any illegal behaviour directed at employing electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers illegal behaviour committed using, or concerning, a computer system or network, including such crimes as unlawful possession and offering or distributing information utilising a computer system or network.[42] One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[43]

It is submitted that cybersecurity is any effort, scheme, venture or activity backed by law, which protects and preserves the confidentiality, integrity, and availability of information, data, and privacy of consumers and ensures security in cyberspace. This definition includes legal measures, policies, security safeguards, risk management approaches, or any other process to secure cyberspace and gain the trust of internet users. Several variables or factors influence and challenge cybersecurity; the factor that affects cybersecurity the most is cybercrime. Cybercrime influences cybersecurity because cybercrime occurs every time cybersecurity is breached. In other words, cybercrime is the repercussion or result of a cybersecurity failure.

1.4 CYBERLAW

Challenges and apprehension surrounded the call for internet regulation. John Perry Barlow's declaration somewhat captures the reservations of multiple netizens who believed that cyberspace was

---

41 Crimes related to computer networks, Background paper for the workshop on crimes related to the computer networks, 10th UN Congress on the Prevention of Crimes and the Treatment of Offenders, 2000, A/CONF.187/10, page 5, <www.uncjin.org/Documents/congr10/10e.pdf> last accessed 16 August 2021.

42 Ibid.

43 Goodman, 'Why the Police Don't Care About Computer Crime' [2000] (10)(3) *Harvard Journal of Law & Technology* 466.

outside the borders of rule-making institutions in the terrestrial world.[44] The declaration came a day after the US Congress enacted the *Communications Decency Act of 1996*, the US first federal shot at regulating internet content. Barlow's declaration stated thus:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone, you are not welcome among us. You have no sovereignty where we gather... Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders.[45]

Early cyber law questions were perceived as a resolution in the twenty years since the rise of cyberlaw.[46] Barlow and other agitators opined that cyberspace is independent with no determinable borders, which justifies their argument that it should not be regulated. The likes of Post and Johnson posited that cyberspace is a distinct environment deserving its own legal framework.[47]

Calo opines that the internet has three hallmarks. The first is that it permits promiscuous and interactive flow. Two, the internet generates shared objects and spaces, that is, collaboration through technology. Finally, the internet allows further alterations and manipulations than offline human control.[48] The law found the extent and affordability of interconnectivity of the internet as challenging.

---

44 Michael Geist, 'Cyberlaw 2.0" (44)(2) Boston College Law Review http://lawdigitalcommons.bc.edu/bclr/vol44/iss2/3.

45 John Perry Barlow, A Declaration of the Independence of Cyberspace [8 February 1996] <http://www.eff.org/-barlow/Declaration-Final.html> accessed 1 August 2021.

46 Ryan Calo, 'Robotics and the Lessons of Cyberlaw' [2015] 103 CALIF. L. REV 513, https://digitalcommons.law.uw.edu/faculty-articles/23 accessed 8 August 2021.

47 David R Johnson and David Post, Law and Borders: The Rise of Law in Cyberspace, [1996] 48 Stan. L., Rev 1367.

48 Calo, (n 46).

In the early 2000s, legal commentators, academics, legal practitioners, and policymakers argued that cyberlaw deserves special scholarly attention as a new field of law/discipline deserving of courses textbooks and professional treatises.[49] Cyberlaw is any rule or regulation that governs cyberspace.[50] It is the law regulating the use of information and communication technology and the internet. It 'deals with codified rules that govern the exchange of communication and information for the protection of intellectual property rights, freedom of speech and public access to information in cyberspace'.[51] Singh et al views cyber law as an effort to apply laws proposed for the physical world to human activity on the internet.[52] The role of cyberlaw is encapsulated thus:

> Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigate and/or prevents harm to people, data, systems, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilities cooperation between countries on cybercrime matters.[53]

In essence, cyberlaw includes substantive, procedural and preventive law. It provides rules of conduct and standard of behaviour regarding

---

49 Ibid.

50 Pooja Aggarwal, P Arora .and R Ghai, 'Review on Cyber Crime and Security' [2014] (2) (1) International Journal of Research in Engineering and Applied Sciences, 48.

51 Umejiaku Nneka Obiamaka & Anyaegbu Mercy Ifeyinwa, 'Legal Framework for the Enforcement of Cyber Law and Cyber Ethics in Nigeria' (15)(10) International Journal of Computer & Technology, 7130.

52 Manjeet Singh, Jacob Anwar Husain & Navneet Kumar Vishwas, 'A Comprehensive Study of Law and Cyber Crimes' [2 February 2014] (3) (2) IJIEASR, 20.

53 'Cybercrime Module 3 Key Issues: The Role of Cybercrime Law' <https://www.unodc.org/e4j/en/cybercrime/module-3/key-issue/the-role-of-cybercrime-law.html> accessed 8 October 2021.

the use of the internet, networks, computers, and related electronic technology to reduce harm and crime in the cyber ecosystem. Cybercrimes, an unlawful act, should be explicitly defined and prohibited by a substantive law of each jurisdiction. The procedural aspect of cyberlaw should lay down the processes and procedures in following the substantive law and the mode of enforcing the substantive law. The preventive law concentrates on legislation seeking to prevent or reduce cybercrime.[54]

Cyberlaw is a constantly evolving discipline. Technology never stands still; instead, it ceaselessly develops and shapes society. The law always struggles to catch up. Each year, numerous jurisdictions contribute to the growth of cyber jurisprudence. There is constantly a new law or updated law in the cyber realm globally. The frequent review and update of cyber laws are due to the uniqueness and diversity of cybercrimes. Cyberlaw is a crucial discipline that should be introduced in tertiary institutions in Nigeria.

1.5 CRUCIAL MILESTONE IN THE GROWTH OF CYBERCRIME

The advent of every new technology and application is accompanied by criminal opportunities exploited immediately.[55] Generally, technology has been used to commit sophisticated crimes. The dawn of new technology has brought faster means of committing crimes. For instance, in the nineteenth century, the development of the telegram attracted the interception of telegraphic communications and the transmission of false information. Its use followed the introduction of the telephone in furtherance of criminal conspiracies.[56]

The milestones in the growth of cybercrime have been alarming. It is difficult to ascertain when the first act of cybercrime occurred

---

54 Ibid.

55 Grabosky, (n 17).

56 Ibid. By the 1970s telecommunications technology allowed one to whistle into a telephone and obtain a free connection, a practice called "phreaking".

with exactitude.[57] However, there are crucial milestones in the history of cybercrime that are noteworthy. One of the highest profiled banking cyber crimes occurred in three years, beginning in 1970.

The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts.[58] Roswell Steffen allegedly stole the money within three years and was never discovered because bank officials asserted that he utilised the computer, which they termed the cleverest and most invisible device available, to conceal his thefts. In 1971, Bob Thomas, a Bolt, Beranek, and Newman (BBN)[59] Technology engineer, developed the first computer creeper virus.[60]

The virus was an experimental self-replicating program that infected other computer systems. It was not destined to damage computer systems but to demonstrate a mobile application.[61] The creeper is regarded as the first computer worm since the computer virus could self-replicate over a computer network like the internet.

In 1977, a programmer based in the Rotterdam offices of Imperial Chemical Industries (ICI) stole hundreds of original computer tapes and their back-ups. The perpetrator and his accomplice attempted

---

57 This is because of the dearth of information gathering of cybercrime. Also, there are dissenting views on what conducts amounts to cybercrime in the past.

58 Lacey Fosburgh, 'Chief Teller is Accused of Theft of $1.5-Million at a Bank Here' *The New York Times* <*https://www.nytimes.com/1973/03/23/archives/cgief-teller-is-accused-of-theft-of-15million-at-a-bank-here-teller.html*>accessed 4 October 2021.

59 The company is a high-technology company based in Cambridge, Massachusetts. It played an extremely important role in the development of packet switching networks and the internet.

60 Police National Legal Database (PNLD) and Andrew Staniforth, *Blackstone's Handbook of Cyber Crime Investigation*,. BabakAkhgar and Francesca Bosco, eds (New York: Oxford University Press 2017) 5.

61 'History of Computers and Computing, Internet, Birth, First Computer Virus of Bob Thomas' <*http://history-computers.com/internet/Maturing/Thomas.html*>accessed 2 October 2021.

to extort ICI by requesting £275,000 for the stolen files.[62] In 1982, the Central Intelligence Agency (CIA) in the US succeeded in finding a way to disrupt the operation of the Siberian gas pipeline in Russia. It was done without using traditional explosive devices. Instead, they caused the Siberian gas pipeline to explode using a portion of a code in the computer system that controlled its operation in what they tagged as a 'logic bomb'. In 1983, a 19-year-old University of California, Los Angeles (UCLA) student used his computer to enter the Defence Department's international communication system.[63]

On 2nd November 1988, Robert Morris released the first intentional hostile computer worm, and within 24 hours, it had caused damage across the world.[64] The worm spread via the internet and infected thousands of systems. The release marked a new dawn for malicious software.[65] In 1994, some Russian-based hackers made 40 transfers totalling $10 million from Citibank to Russian, Germany, Finland, the US, Netherlands, and Switzerland.[66] Between 1995 and 1998, the Newscorp pay-to-view encrypted SKY-TV suffered several hacking attacks during an ongoing technological arms race between the Pan-European hacking group and Newscorp.[67]

The original motivation of the hackers was to watch Star Trek re-runs in Germany, even though Newscorp did not have the copyright to allow them to do so. Between 1995 and 1998, a group of Nigerian fraudsters, Emmanuel Nwude, Ikechukwu Anajemba and Amaka Anajemba, collaborated with some Asians involved in financial crime, termed the largest scam of its type in Nigeria and the third biggest

---

62 PNLD and Andrew Staniforth, (n 60).

63 Henry Pontell, 'Identity Fraud, Cyber-Crime, and White-Collar Delinquency' *<http://www.austlii.edu.au/journals/AdelLawRw/2002/17.pdf>* accessed 9 October 2021.

64 Sebastian Bortnik, 'Five Interesting Facts about the Morris Worm (for its 25th Anniversary)' [6 November 2013] <http://www. welive security.com> accessed 2 October 2021.

65 Ibid. He was arrested by the US authorities and sentenced to 3 years' probation, 400 hours of community service and a fine of $10,000.

66 PNLD and Andrew Staniforth, (n 60).

67 'Documented Cases of Cybercrime one of the Highest' *<https://www.coursehero.com>* last accessed 2 October 2021.

private scam in documented history.[68] The perpetrators defrauded and looted Nelson Sakaguchi and a Brazilian bank, Branco Noroeste Brazil, $224 million, leading to the Bank's liquidation.[69]

In 2000, a series of denial-of-service attacks against high profile websites, including Yahoo! eBay, Amazon, Dell, E*TRADE and CNN, began courtesy of an individual under the alias of Mafiaboy.[70] Computers at the University of California and about 50 computers at Stanford University were among the zombie computers sending pings in DDoS attacks.[71] In 2008, Sergei Tsurikov, an Estonian national, conspired with a group of people to hack into the computer network of RBS Word Play.[72]

The attackers succeeded in compromising the data encryption used by RBS and raised the account limits on payroll debit cards. They created forty-four counterfeit payroll debit cards and provided a network of cashers, and these cards were used to withdraw over $9 million from 2,100 ATMs in at least 280 cities worldwide.[73] In October 2014, Tsurikov was sentenced to eleven years imprisonment for his conspiracy, resulting in the loss of over $9.4 million.[74]

---

68 'How Emmanuel Nwude sold an Imaginary Airport for 242 Million Dollars' <*https://www.pulse.ng/gist/yahoo-boy-no-laptop-how-emmanuel-nwude-sold-an-imaginery-airport-for-242-million/8lgmq1v*>last accessed 14 August 2021.

69 Nwude and Ikechukwu Anajemba impersonated the CBN Governor and CBN's Director of International Remittance respectively. With the use of false correspondence and high-level documents they were able to convince Sakaguchi that the Nigerian government was seeking for investors to build an airport in Abuja. They deal was that if Sakaguchi could provide the first investment, which was the sum of $ 242 million dollars, he would be entitled to 10% of that amount.

70 PNLD and Andrew Staniforth, (n 60).

71 In August 2000, the Canadian federal prosecutors charged Mafiaboy with 54 counts of illegal access to computers and 10 counts of mischief to data for his attacks.

72 Jonathan Clough, *Principles of Cybercrimes* (2nd ed United Kingdom: Cambridge University Press, 2015) 3.

73 Including cities like US, kraine, Russia, Estonia, Japan, Italy and Canada.

74 US Department of Justice, 'International Hacker Sentenced', Press Release (24 October 2014) cited in Clough, (n 50).

In 2010, Nikita Kuzmin, a Russian national, created the Gozi virus.[75] The virus infected over one million computers globally and caused tens of millions of dollars in losses.[76] The virus was described as one of the most financially destructive computer viruses in history. The virus creator and two other individuals who played vital roles in creating and distributing the virus were arrested in the US on different dates.[77] In 2014, Sony Pictures, a major entertainment company, was hit by a crippling virus.[78] A cybercrime group called Guardians of Peace (GOP) was behind the alleged blackmail attempt, which saw about 100 terabytes of sensitive data stolen from the company.[79] In 2015, almost 157,000 TalkTalk customers had their personal details hacked.80 TalkTalk revealed that the total number of customers affected by the attack was 156,959, including 15,656 whose bank account numbers and sort codes were attacked.

In 2017, the Wannacry virus infiltrated the National Health Services computer system in the UK.[81] For almost one week, computer systems were disabled, forcing hospitals and medical

---

75 'Three Alleged International Cyber Criminals Responsible for Creating and Distributing Virus that Infected Over One Million Computers and cause Tens of Millions of Dollars in Losses Charged in Manhattan Court' <https://www.justice.gov/usao-sdny/pr/three-alleged-international-cyber-criminals-responsible-creating-and- distributing-virus>accessed 4 October 2021.

76 NASA computers were among the 40,000 US computers infected with Gozi virus.

77 Ibid.

78 Dan Elson, 'Attack of the Hack: Five of the Worst Cases of Cyber Crime the World has ever Seen- from Data Theft of One Billion Yahoo Users to Crippling the NHS' [11 October 2017] https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-nhs/ accessed 3 October 2021.

79 Ibid.

80 Sean Farrell, 'Nearly 157,000 had Data Breached in TalkTalk Cyber-Attack' [6 November 2015] <https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack/>accessed 1 October 2021.

81 PNLD and Andrew Staniforth, (n 60).

practitioners to operate offline.[82] Also, in 2017, two Nigerians and six other persons were involved in a series of intrusions into the servers and email systems of a Memphis- based real estate company. They identified large financial transactions by spoofing email addresses and other anonymisation methods. They set up a fraudulent email correspondence with the Company's business parties and redirected funds for real estate transactions to destinations in Africa.

In 2019, an international cybercrime gang infected computers with the GozNym[83] malware obtained online banking details to access numerous bank accounts. They succeeded in stealing $100m (One Hundred Million Dollars) from more than 40,000 (forty thousand) victims.[84] Investigations were conducted in the US, Bulgaria, Germany, Georgia, Moldova, and Ukraine by a complex police operation. Ten gang members have been charged in Pittsburgh, US, for laundering funds using the US and foreign accounts, amongst other cybercrimes. Five Russian nationals who are members of the network remain on the run, including the malware developer.[85]

In August 2019, the US Federal Bureau of Investigation (FBI) publicised a list of suspects involved in one of the largest scams in US history. It announced charges against 80 suspects, of which 77 were Nigerians, in a wide-ranging $46 million internet scam.[86] In a

---

82 Ibid.

83 GozNym is a hybrid of nymaim and gozi, two pieces of malware. Nymaim also known as dropper, is a software designed to sneak other malware on to a device and install it. While gozi, which has been around since 2007 resurfaced with new techniques all aimed at stealing financial information. It has been used severally in concerted attacks on US banks.

84 Jane Wakefield 'GozNym Cyber-Crime Gang which stole Millions Busted-BBC News' [16 May 2019] <https://www.bbc.com/news/technology-48294788> last accessed 1 October 2021.

85 Ibid.

86 'US Charges 80 People, Mostly Nigerians in $46m Internet Scam' [23 August 2019] <https://www.aljazeera.com/news/2019/08/charges-80-people-nigerians-46m-internet-scam-190823071850782.html> last accessed 26 September 2021.

252-count federal grand jury indictment, the defendants were accused of partaking in numerous fraud schemes, including conspiracy to commit wire fraud, mail fraud, bank fraud, and money laundering through a Los Angeles-based network.[87] On 22nd August 2019, 14 out of the 80 suspects were arrested in raids carried out across the US. The Economic and Financial Crimes Commission is working with the FBI to arrest and extradite the Nigerian- based accomplices to the US to face justice.[88]

In 2020, the United Arab Emirates investigators arrested Ramon Olorunwa Abbas, known as Ray Hushpuppi, a Nigerian national, and handed him to FBI agents. Federal prosecutors alleged that Huspuppi led a global network that defrauded hundreds of millions of dollars from companies through business email compromise schemes, computer intrusion, and money laundering.[89] Amal Al Jallaf, director of the criminal investigative department of Dubai Police, stated that Hushpuppi flaunted his extravagant lifestyle via social media under a businessman façade in an attempt to lure victims from over the world.[90] Officers indicated that they found the email addresses of almost two million victims on dozen phones, hard drives and computers. The preceding is a tiny percentage of crimes

---

87 '77 Nigerians Implicated in one of the Largest Fraud Cases in US History' [22 August 2019] <https://www.pulse.ng/news/local/us-charges-dpzens-of-Nigerians-with-fraud-in-massive-bust/qv6mcxp> accessed 26 September 2021.

88 FBI 419 List: We'll Handover Indicted Nigerian-Based Suspects to FBI-EFCC' [29 August 2019] <https://huhuonline.com/> last accessed 2 October 2021.

89 'Nigerian National Brought to U.S to Face Charges of Conspiring to Launder Hundreds of Millions of Dollars from Cybercrime Schemes' [3 July 2020] <https://www.justice.gov/usao-cdca/pr/nigerian-natiobal-brought-us-face-charges-conspring-launder-hundreds-millions-dollars> accessed 1 October 2021.

90 Matt Mathers, 'Instagram Influencer 'Hushpuppi' arrested Amid Claims of E350 Million Global Cyberscam' [29 June 2020] <hhtps://www.independent.co.uk/news/world/middle-east/huspuppi-instagram-news-arrested-cyberscam-350-million-a9590826.html> accessed 1 October 2021.

Commission headings of fraud, theft, unauthorised private work, misuse of personal data, sabotage and pornography into the computer- assisted category. While hacking and viruses fall into the category of computer-focused crime.[94]

Eoghan Casey's definition of computer crime has been described as a valuable means of classifying cybercrime.[95] He defined a computer crime as a crime that involves a computer in one of the following ways: The computer as an instrument of crime. Here, the computer is used as a means of engaging in criminal activity. Under this category, the crime cannot be committed without the computer being turned on and used in the commission of the act. The computer as the focus of a crime. Here, the computer is the intended target of criminal activity and is not necessarily used in the commission of the act. The computer as a repository of evidence. Here, the individual involved in a criminal act has not stolen the computer and has not used the computer as a means of committing the criminal act, but he or she has stored evidence on the machine.

This definition encapsulates when the computer is used as an instrument to perpetrate crime, the focus of the crime and used as a storage device.[96] Cybercrime has also been classified as cyber-dependent and cyber- enabled crimes. Cyber-dependent crimes are offences that can only be committed using computers, computer networks, or any other form of ICT.[97] Acts like the spread of viruses and other malicious software and hacking come within the ambit of cyber-dependent crimes. Such crimes are acts primarily directed against computers or network resources, although there may be secondary outcomes from such attacks, such as fraud.

On the other hand, cyber-enabled crimes are traditional crimes that are amplified in their extent or scale by the use of computers,

---

94 Ibid.

95 Ifeoma E Nwafor, 'Cybercrime in Nigeria: The Role of Internet Service Providers in Enhancing Cybersecurity' (Emerging Challenges of Cybersecurity Warfare and Countermeasure, Southeast Cybersecurity Conference & Exhibition 2018).

96 ibid.

97 PNLD and Staniforth, (n 60) 12.

committed in cyberspace. Daily news of cybercrimes makes the headlines in newspapers and magazines. Offenders develop strategies to defraud victims using different types of cybercrime.

1.6 CLASSIFICATION OF CYBERCRIME

The classification of cybercrime has taken different forms and standards. There is no consensus on the classification of cybercrime. Scholars and commentators view the categorisation of cybercrime from different perspectives. Grabosky[91] opined that a useful approach would be to differentiate those crimes in which the computer is used either as the instrument to commit the offence, the target of the offence; or incidental to the offence.

He also suggested that cybercrime can be categorised by differentiating between old or conventional crimes committed with new technology; and new crimes that are committed with modern technology. He argues that cybercrimes can be likened to 'old wine in new bottles' because it is similar to terrestrial crimes.[92]

Furnell categorised cybercrime based on the UK Audit Commission's surveys to determine the extent of computer crime and abuse problems in the UK's public and private sectors.[93] He argues that a distinction can be drawn between computer-assisted crimes and those that are computer- focused. He defined computer-assisted crimes as activities/ cases where the computer is used in a supporting capacity. Still, the underlying crime either predates the emergence of computers or could be committed without them. He described computer-focused crimes as activities/ cases in which the category of crime emerged directly from computer technology. There is no direct parallel in other sectors. He categorised the Audit

---

91 Grabosky (n 17).

92 ibid.

93 SM Furnell, 'The Problem of Categorising Cybercrime and Cybercriminals' (Survival in the E-Conomy: 2nd Australian Information Warfare & Security Conference, Perth, Western Australia, 2001) William Hutchinson, M Warren, J Burn (eds) <http://ro.ecu.edu.au/ecuworks/6758>accessed 1 October 2021.

computer networks or other ICT. These crimes can still be committed without the use of ICT, unlike cyber-dependent crimes. Acts like fraud, theft and sexual offences against children are cyber-enabled crimes.[98]

Cybercrime has also been categorised as violent and non-violent crimes.[99] Offences like cyber terrorism, cyberstalking, pornography, and cyberbullying come under cybercrime's violent category. In contrast, offences like cyber theft,[100] cyber fraud, cyber trespass, and destructive cybercrimes[101] come under the non-violent category.[102] The Convention on Cybercrime adopted a different approach to the classification of cybercrime.[103] It distinguishes cybercrime between four different types of offences.[104] These are:

i. Offences against the confidentiality, integrity, and availability of computer data and systems;[105]
ii. Computer-related offences;[106]
iii. Content-related offences;[107] and
iv. Copyright-related offences.[108]

---

98 Ibid.

99 'Cybercrime: A Conceptual and Theoretical Framework' <*http://shodganga.inflibnet.ac.in>bitstream*> last accessed 1 October 2021.

100 This includes embezzlement, unlawful appropriation, corporate espionage, plagiarism, piracy, identity theft etcetera.

101 This includes cyber vandalism and viruses.

102 'Cybercrime: A Conceptual and Theoretical Framework' (n 83).

103 Council of Europe Convention on Cybercrime (CETS No. 185) <*http://conventions.coe.int.*> last accessed 2 October 2021.

104 M Gercke, 'Understanding Cybercrime: A Guide for Developing Countries' [March 2011] *International Telecommunication Union Cybercrime Legislation Resources* <*http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html*> last accessed 2 October 2021.

105 Art 2 (illegal access), Art 3 (Illegal interception), Art 4 (Data interference), Art 5 (System interference), Art 6 (Misuse of devices) etcetera.

106 Art 7 (Computer-related forgery), Art 8 (Computer-related fraud) etcetera.

107 Art 9 (Offences related to child pornography).

108 Art 10 (Offences related to infringements of copyright and related rights).

In summary, the Convention categorised cybercrime into offences against the confidentiality, integrity, and availability of computer systems and other classes of acts considered as a misuse of computer systems or networks. The classifications of cybercrime provided by various scholars are relevant when viewed in isolation. Each scholar categorises it from their perspective. In an attempt to compare the multiple classifications offered by scholars, it shows most of these classifications overlap, and they are variable. It is submitted that the absence of an unambiguous and generally accepted definition and classification of cybercrime serves as a handicap in investigating and prosecution of cybercrime.

1.7 TYPES OF CYBERCRIME

Numerous activities amount to cybercrime, owing to the medium in which it was committed, the offence's target, or the environment where it was committed (virtual). The typology of cyber-dependent crimes and cyber-enabled crimes will apply in this section of the book. Subsequently, the various types of cybercrime that come under each category will be discussed briefly. This approach is adopted because it categorises cybercrimes for easy apprehension.

1. Cyber-dependent Crimes

Cyber-dependent crimes can only be perpetrated using a computer, computer networks or any other form of Information Communications Technology (ICT).[109] Simply put, cyber-dependent crimes occur when an electronic system is the medium and the target of a cyber-attack. It could be carried out by illegal invasions into computer networks or by disrupting a computer's functionality or network.

There are various types of cybercrime that come under this category. These include:

---

109 Mike McGuire and Samantha Dowling, 'Cyber Crime: A Review of the Evidence' [October 2013] *Research Report* 75 <*http://assets.publishing.service.gov.uk*> last accessed 1 October 2021.

a Hacking

Hacking is a form of trespass whereby the perpetrator gains unauthorised access into a computer or network by exploiting identified security vulnerabilities in such a system.[110] It has been defined 'as any technical effort to manipulate the normal behaviour of a computer, computer network connections and connected systems'.[111] It has been described as one of the most extensively evaluated and debated forms of cybercriminal activity.[112] Grabosky[113] defined hacking as '...the unauthorised access to a computer or computer system'. In most cases, hacking is used to gather personal data, deface websites, or be employed as part of the denial of service or distributed denial of service.

b. Denial of Service

A denial-of-Service (DoS) attack is an act or attack which intends to shut down a machine or network, making it inaccessible to the intended users.[114] The shutdown is accomplished by flooding the target's device with traffic or sending information that triggers a crash. In such an attack, the attacker uses up all available resources to the server and denies the legitimate user(s) basic service.[115]

c Distributed Denial of Service

In a Distributed Denial of Service (DDoS) attack, the legitimate user is denied access or services available on the affected computer due to attacks from multiple computers.[116] The attacker targets the device and its network connection and prevents the

---

110 Ibid.

111 PNLD and Staniforth, (n 60) 13.

112 Ibid.

113 Grabosky, (n 17).

114 What is Denial of Service Attack (DoS)?' <*http://www.paloaltonetworks.com*> last accessed 2 October 2021.

115 GU Devi, MK Priyan, EV Balan, CG Nath, M Chandrasekhar, 'Detection of DDoS Attack using Optimized Hop Count Filtering Technique' [26 October 2015] *India Journal of Science & Technology* 8(26) <*http://www.indjst.org*>accessed 2 October 2021.

116 PNLD and Staniforth, (n 60) 12.

user from accessing information or services.[117] It is important to note that DDoS attacks do not entail the perpetrator gaining access to the computer. Instead, the perpetrator intends to prevent the user from accessing information by disrupting network of website availability as the case may be.

d. Malware

Malware is a portmanteau term for malicious software that spreads between computers and interferes with its operations.[118] There are various forms of malware; these are:

i. Viruses

A virus is a computer program that can copy itself and infect computers.[119] It can cause a mild dysfunction in a computer system. In severe cases, its effects can result in damaging or deleting hardware, software or files. Viruses are self-replicating programs that spread within and between computers. They cannot infect a computer without a host, that is, human action. This means that a host is required to run or open the infected file. It is likened to a biological virus that requires a human host to facilitate the spread of the infection.

ii. Worms

Worms are self-replicating programs that can spread independently, within and between computers, without a host or human action. The effect of worms is usually more severe than that of viruses, destroying the whole network.[120] Worms and viruses are both self- replicating programs. The difference between the two malware is that, unlike viruses, worms can spread to other computers or networks without a host or human action.

iii. Trojans

Trojans are a form of malware that appears as a legitimate

---

117 Susan W Brenner, *Cybercrime and the Law*, (Boston: Northeastwestern University Press 2012) 45.

118 McGuire and Dowling, (n 109).

119 Brenner, (n 117) 16.

120 Ibid.

program but facilitates illegal access to a computer device. The term originates from the classical myth of the Trojan horse.[121] It usually appears as a harmless or innocent program, but it contains hidden functions.[122] Such programs may be embedded in email attachments, software, or websites. For example, Financial Trojans may scan for the URLs of common financial institutions, performing 'Man-In-The-Browser' (MITB) attacks during online banking sessions. Malicious banking apps for mobile phones is a familiar medium used to deliver banking Trojans. Such apps intercept and send SMS messages to acquire information stored on the mobile device.[123] Victims fall prey to such malicious programs because it is disguised as a legitimate website, software, or app as the case may be.

iv. Spyware

Spyware is a type of software used to invade users' privacy by gathering sensitive or personal information from infected systems and monitoring the websites visited.[124] They are applications tailored to amass information of an individual or organisation without their knowledge or approval. In some cases, users install spyware on their system or network by downloading materials from the web or visiting a dubious website.

v. Bots

A bot is a program that infects a targeted computer intending to control it remotely. Bots known as internal robots are used to gain total control over a computer/ network.[125] Unknown to a user, the attacker employs the small programs called 'daemons' that run in the host computer's background

---

121 Mark Cartwright, 'Trojan War: Ancient History Encyclopaedia' [22 March 2018] <*https://www.ancient.eu/Trojan_War/*> last accessed 26 September 2021.

122 Clough, (n 72) 40.

123 Ibid.

124 Brenner, (n 117) 31.

125 'What are Bots?' <*https://us.norton.com/internetsecurity-malware-what-are-bots.html*>last accessed 14 September 2021.

program but facilitates illegal access to a computer device. The term originates from the classical myth of the Trojan horse.[121] It usually appears as a harmless or innocent program, but it contains hidden functions.[122] Such programs may be embedded in email attachments, software, or websites. For example, Financial Trojans may scan for the URLs of common financial institutions, performing 'Man-In-The-Browser' (MITB) attacks during online banking sessions. Malicious banking apps for mobile phones is a familiar medium used to deliver banking Trojans. Such apps intercept and send SMS messages to acquire information stored on the mobile device.[123] Victims fall prey to such malicious programs because it is disguised as a legitimate website, software, or app as the case may be.

iv. Spyware

Spyware is a type of software used to invade users' privacy by gathering sensitive or personal information from infected systems and monitoring the websites visited.[124] They are applications tailored to amass information of an individual or organisation without their knowledge or approval. In some cases, users install spyware on their system or network by downloading materials from the web or visiting a dubious website.

v. Bots

A bot is a program that infects a targeted computer intending to control it remotely. Bots known as internal robots are used to gain total control over a computer/ network.[125] Unknown to a user, the attacker employs the small programs called 'daemons' that run in the host computer's background

---

121 Mark Cartwright, 'Trojan War: Ancient History Encyclopaedia' [22 March 2018] <*https://www.ancient.eu/Trojan_War/*> last accessed 26 September 2021.

122 Clough, (n 72) 40.

123 Ibid.

124 Brenner, (n 117) 31.

125 'What are Bots?' <*https://us.norton.com/internetsecurity-malware-what-are-bots.html*>last accessed 14 September 2021.

to exploit security weaknesses.[126] The host computer is referred to as 'zombie' or 'bot', and these botnets can be instructed to perform coordinated tasks. Botnets are exceptionally versatile and may be involved in a range of other cybercrimes.

2. Cyber-enabled Crimes/ Computer as a Tool to Commit a Crime

Cyber-enabled crimes are traditional/existing crimes that have been increased in scale or transformed by using computers, computer networks, or other ICT forms. It is important to note that cyber-enabled crimes do not solely depend on computers or computer networks. However, the scale and style of committing them are transformed by the use of digital technology. For instance, fraud has been in existence for a very long time, but how it is presently perpetrated has changed, and the scale of online fraud has drastically proliferated. Cyber-enabled crimes fall into the following categories:

i. Economic-related Cybercrimes/Unauthorised Alteration of Data

Economic-related cybercrimes are offences perpetrated online by illegally altering data or information for personal or organisational gain. It includes the following crimes:

a. Online/Cyber fraud: Online/cyber fraud is discussed somewhat extensively because this book is centred around it. Fraud is the erroneous representation utilising a declaration or conduct made knowingly or recklessly to gain material gain'.[127] Cyber fraud is defined broadly as any fraud perpetrated with the medium or aid of online programming or cyber-related communications such as email, websites, and chatroom.[128] Numerous cyber frauds and scams are committed daily in cyberspace. Some of the

---

126 Clough, (n 72) 41.

127 Majid Yar, *Cybercrime and Society*, (2nd ed London: SAGE Publications Ltd 2013) 79.

128 Financial Times [24 April 1997] cited in Amita Verma, 'Cyber Fraud: A Digital Crime' *IADIS International Conference Information Systems 2008* <*https://www.academia.edu*>last accessed 1 October 2021.

most common forms of cyber fraud are website design scams, multi-level marketing schemes, ISPs scams, fraudulent investment scams, online auction, etcetera.[129] The use of email has been instrumental in the online fraud boom. It has been an inexpensive medium for sending convincing messages to millions of prospective victims.[130] It does not cost much, and it is easy to use. Cyber fraud perpetrators compose persuasive messages using well-known brands or icons that fool meticulous or internet-savvy users.

The rate of online/cyber fraud has skyrocketed. The Internet Crime Complaint Centre (IC3)[131] received 288,012 complaints on different forms of cyber fraud in 2015.[132] Approximately 44 per cent of these complaints reported losses of $1 billion. Based on these estimates, the average loss to these victims was $8,421'.[133] It is submitted that these estimates do not fully represent the analysis of internet fraud in cyberspace. This is due to insufficient official data and victims' reluctance to report cyber fraud attacks.

There are different types of fraud. Some of the most commonly committed kinds include Advanced fee fraud or Nigerian scams, Identity theft, email- based scams, cheque fraud, internet auction fraud, ATM fraud, romance scams, charity fraud, credit card fraud, and website fraud misdirection and work-from-home scams, etcetera. This section will discuss two forms of fraud, these are:

---

129 Ibid.

130 Thomas J Holt, Adam M Bossler and Kathryn C Seigfried-Spellar, *Cybercrime and Digital Forensic*, (2nd edn New York: Routledge 2018) 205.

131 Formerly Internet Fraud Complaint Centre (IFCC)) is an organizational collaboration between the FBI and the National White-Collar Crime Centre (NW3C). The organization's key role is to receive public reports of cybercrime and refer them to the pertinent criminal justice agencies for appropriate action.

132 Holt and others, (n 130).

133 Ibid.

a. Advance Fee Fraud or Nigerian Scam

Advanced fee fraud, also known as Nigerian scam, or '419 fraud', was named after section 419 of the Criminal Code, which prohibits and prescribes punishment for obtaining property by false pretences.[134] The infamous advanced fee fraud scheme originated in Nigeria and has spread around the world.[135] Grabosky[136] is of the view that the Nigerian scam is one of the most common forms of fraud. Nigerian scams can be broadly described as an act where a Nigerian offers a person residing abroad a share in a large sum of money or a payment on the condition that the person transfers money out of their country.[137] The potential victim is usually contacted by mail, text message, social media, and phone calls.

In most cases, the communication emanates from a person who purports to be a current or former government official. It informs the potential victim of a fortune, usually ill-gotten, deposited in a Nigerian bank account and cannot be safely extracted due to political turbulence. So, a trustworthy foreigner's account is needed for the funds' transfer in exchange for a substantial percentage of the fund.[138] Another variation of this scam involves the scammer purporting to be a wealthy heir to a deceased person who craves assistance moving the inherited funds out of the country.[139] The sender defrauds a potential victim by asking for a small donation to get an account or fund out of the holding process.[140] The scammer keeps asking for funds to resolve complications in obtaining their account or legal

---

134 See Criminal Code Act, s 419.

135 'What is the Nigerian Scam (419 scam)' <*https://www. fight identity theft. com/ internet _ scam _ nigerian. html*>last accessed 1 October 2021.

136 Grabosky, (n 17). '419 fraud' is an updated version of the Spanish prisoner and dates back to 1588.

137 'Nigerian Scams' <*https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams*> last accessed 17 October 2021.

138 Brenner, (n 117).

139 Holt and others, (n 130).

140 The FBI and the IC3 Internet Crime Report reported that Americans lost about $58 million to Nigerian scam in 2017.

fees needed to move the account.[141] The victim gives substantial sums repeatedly. This process continues until the victim is no longer willing to pay or the scammer simply disappears.

In summary, the Nigerian scam involves the following elements: a communication (email, text message, etcetera) from a person in another country; an intention to transfer money out of his country; messages asking for funds to speed up the transfer or pay legal fees and an offer of financial reward from the share of the fund to the receiver of such message.

b. Identity Fraud

Identity fraud is the wrongful obtainment and use of another person's data in ways that involve fraud or deception, typically for economic gain.[142] With the information obtained, the perpetrator takes over the individual's identity to conduct various crimes.[143] Identity theft is the unlawful use and possession of personally identifiable information of another person with the intent to commit, aid, or abet illegal activity.[144]

Other categories of cybercrime include:

3. Malicious and Offensive Communications

Malicious and offensive communication is any form of communication that is grossly offensive or indecent, menacing or contains information that is false or believed to be false.[145] Section 1

---

141 Ibid.

142 'Identity Theft/CRIMINAL-FRAUD/Department of Justice' <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> last accessed 2 October 2021.

143 Ibid. for instance, fraudulent withdrawals from banks accounts, false applications for loans and credit cards. See *United States v Godin* 534 F 3d 51 and *State v Baron, 2008 WL 2201778* (Wisconsin Court of Appeals).

144 Holt and others, (n 130).

145 West Midlands Police 'Malicious Communications' *<https://west-midlands.police.uk/your-options/malicious-communications>*

of the *Malicious Communications Act*[146] of the UK defined malicious communication as:

(1) any person who sends to another person-

(a) a letter, electronic communication or article of any description which conveys-

(i) a message that is indecent, grossly offensive;

(ii) a threat; or

(iii) information which is false and know or believed to be false by the sender; or

(b) Any article or electronic communication which is, in whole or in part, of an indecent or grossly offensive nature; is guilty of an offence if his purpose, or one of his purposes, in sending it is... to cause distress or anxiety to the recipient or to any other person to whom he intends that, or its contents or nature should be communicated.

The sender of such a message intends to cause distress or anxiety to the recipient. The offence occurs as soon as the communication is sent. It is irrelevant whether the intended recipient received the communication or not.[147] Other offensive and malicious communications include communication sent via social media, cyberbullying/ trolling, and virtual mobbing.

4. Content Violations

Content violations include copyrights crimes, intellectual property, hate crimes, harmful contents, child pornography, military secrets and forgery/ counterfeit.

---

146 Malicious Communications Act 1988.

147 Ibid.

5. Offences that specifically target individuals.
Offences targeting individuals include Cyber-Enabled Violence against Women and Girls (VAWG), cyberstalking and harassment, and revenge pornography.

6. Online Child Sexual Offences.
This offence includes child sexual abuse, online grooming, prohibited and indecent images of children.[148]

---

148 'Cybercrime Prosecution Guidance/The Crown Prosecution Service' <*https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance*>last accessed 17 September 2021.