Cavendish University Law Journal Vol. 1 August 2022

AN ANALYSIS OF THE NATURE AND SCOPE OF CYBERCRIME

CULJ

ISSN 2957-8647

Volume 1

pp. 179-193

August 2022

www.cavendish.ac.ug

Email: secretaryculj@cavendish

Peter Ter Ortese*

Abstract

Cybercrime have become sophisticated and growing rapidly across multiple jurisdictions encompassing all forms of criminal activities through the use of computer and the internet. Cybercrimes are carried out through illegal access into the computer database; illegal interception of data, data interference, system, interference, misuse of devices, forgery and other forms of electronic scam. This paper indicates that there is lack of a globally acceptable definition of cybercrimes because of the definitional changes depending on the purpose in which the definition is used. The paper further argues that categorizing the offence of cybercrime often leads to confusion and differences in nomenclature. Some countries or jurisdiction define or categorize cybercrime as a means of using it to fight a particular criminal activity thereby making the said criminal activity punishable in their jurisdictions. This paper concludes that unless there is a workable definition of cybercrimes, different authors and even international bodies and jurisdictions will continue to define cybercrime based on their perceptions. The paper therefore, recommends a workable definition and an identifiable and clear-cut categorization of cybercrime devoid of controversy.

* LLB (Hons), BL, LLM, PhD Student University of Uyo, Akwa Ibom State, Nigeria and Divisional Registrar, National Industrial Court of Nigeria, Uyo Division Email: peterortese@gmail.com Tel. No.:08035446931

Introduction

This paper considers definitional matters, nature and scope of cybercrime. It highlights some of the definitional challenges of cybercrime. It begins with a premise of the challenges of arriving at a precise definition or lack thereof of cybercrime. Hence various approaches have been adopted in recent decades to develop a precise definition of the term "computer crime" and "cybercrime" Cybercrimes have become sophisticated and growing rapidly across multiple jurisdictions encompassing all forms of criminal activities through the use of computer and the internet. Cybercrimes are carried out through illegal access into the computer database; illegal interception of data, data interference, system, interference, misuse of devices, forgery and other forms of electronic scam. There is lack of a globally acceptable definition of cybercrimes because of the definitional changes depending on the purpose in which the definition is used. Categorizing the offence of cybercrime often leads to confusion and differences in nomenclature. Some countries or jurisdiction define or categorize cybercrime as a means of using it to fight a particular criminal activity. Thereby making the said criminal activity punishable in their jurisdiction. There is lack of workable definition of cybercrimes, different authors and even international bodies and jurisdictions have continued to define cybercrime based on their perceptions. The paper therefore examines a workable definition and an identifiable clear-cut categorization of cybercrime devoid of controversy.

Definition and Nature of Cybercrime

Cybercrime is now recognized as a major international problem, with continual increases in incidents of hacking, viruses, and other forms of abuse having been reported in recent years[1]. There appears to be no precise definition for "cybercrime" or "computer crime" according to Boussi and Gupta[2]. Nor does there seem to be a globally accepted standardised definition for cybercrime. However, although many commentators, scholars and experts may recognise cybercrime-related terminology, agreeing and defining what they mean can prove to be somewhat difficult. As a result,

[1]SoumyaTiwari, AnshikaBhalla and RituRawat, "Cyber Crime and Security" (2016) 6 *International Journal of Advanced Research in Computer Science and Software Engineering* 46 <http://ijarcsse.com/Before_August_2017/docs/papers/Volume_6/4_April2016/V6I4-0201.pdf> accessed March 23, 2021.

[2] Grace Odette Boussi and Himanshu Gupta, "A Proposed Framework for Controlling Cyber-Crime," *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (2020) <https://ieeexplore.ieee.org/document/9197975> accessed March 23, 2021.

alternative classifications have emerged from a range of authoritative sources, which are similar in some respects, but markedly different in others.

Pati argues that "cybercrime" is a misnomer and the concept of cybercrime is not different from the concept of conventional crime as both include an act or omission which causes a violation of the law[3]. It was also argued by ShilpaYadav, Tanu Shree and YashikaArora that the term is a misnomer that describes criminal behaviour where the computer or computer networks may be a source, tool, target, or a place of criminal activity[4]. It is imperative to note that the above definition include an act or omission but cybercrime is not contained in the criminal or penal code, therefore, the reference to a conventional crime is uncalled for. Also, the term is used interchangeably with computer crime, electronic crime, high-technology crime, information age crime, cybernetic crime, computer-related crime, or digital crime.[5] This definition is all encompassing, it is not narrow in scope, however not all electronic crimes are computer based. Even the United Nation (UN) uses the terms computer crime and computer-related crime interchangeably[6].The United Nations defines cybercrime in two ways. Narrowly, as the "illegal behaviour directed utilizing electronic operations that target the security of computer systems and the data processed by them"[7] and more broadly defined, cybercrimes are "any illegal behaviour committed utilizing, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information utilizing a computer system or network."[8] It is worthy of note that the earlier definition is narrow while the latter is broad in perspective. The narrow definition limit cybercrime to only illegal behaviour on computer system without recourse to the network system which is fundamental to the commission of cybercrime. The broad definition examine cybercrime as against computer and network. The both definitions however, admit that crime committed on the computer could also be referred to as cybercrime.

At present, when we talk about computer crime or cybercrime, a direct reflection of this is the assumption that computers or networks are involved in this crime.

---

[3]ParthasarathiPati, "Cyber Crime" (*www.naavi.org*2003) <https://www.naavi.org/pati/pati_cybercrimes_dec03.htm> accessed March 24, 2021.

[4]ShilpaYadav, Tanu Shree and YashikaArora, "Cyber Crime and Security" (2013) 4 International Journal of Scientific & Engineering Research 855, 861 <https://www.ijser.org/researchpaper/CYBER-CRIME-AND-SECURITY.pdf> accessed March 23, 2021.

[5]*Ibid*.

[6] United Nations, United Nations Crime and Justice Information Network (United Nations 1999), para. 21

[7] United Nations, "Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders" (United Nations 2000) p. 5 <http://bit.ly/2kjJFXN> accessed March 24, 2021.

[8] Ibid.

The term 'cybercrime' was appositely considered by Sabillion and his colleagues as a series of criminal acts based on the material offence object and modus operandi that affect computer data or systems[9].To Sharma[10], Cybercrime is a crime done with the misuse of information technology for unauthorized or illegal access, electronic fraud; like deletion, alteration, interception, concealment of data, forgery etc. He further noted that the activity of a person would be tagged a "cybercrime" if a computer is either a tool or a target or both. This definition on cybercrime is inclusive as it examines the basic element of cybercrime which involves the computer system and network. The author indicates the various forms of crimes committed through the computer system and the network which therefore, gives an all-encompassing understanding of the concept of cybercrime. Also, following this line of thought, Kshteri defined "cybercrime" as criminal activities in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations.[11] The author's definition seem narrow and ambiguous in perspective. The word criminal activity could give different interpretation and understanding of the concept as it is broad and general to the offence of crime and not narrow down to cybercrime as a focus. The definition seems vague and open ended.

However, Watney[12] had a different opinion or view on the definition wherein he defined "cybercrime" as any unlawful conduct involving a computer or computer system or computer network, irrespective of whether it is the object of the crime or instrumental in the commission of the crime. This view is also adopted by Maitanmi and other colleagues who defined cybercrime as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes.[13] This view of cybercrime is very predominant amongst legal

[9]Regner Sabillon and others, "Cybercriminals, Cyberattacks and Cybercrime," *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (2016) <https://ieeexplore.ieee.org/document/7740434> accessed March 23, 2021.

[10] Kumar Sudhir Sharma, "Cyber Security: A Legal Perspective" (2017) 9 International Journal of Computer and Internet Security 1 <https://www.ripublication.com/irph/ijcis17/ijcisv9n1_01.pdf> accessed March 23, 2021.

[11]NirKshetri, Cybercrime and Cybersecurity in the Global South (Palgrave Macmillan 2013) p. 6

[12] M Watney, "Cybercrime and the Investigation of Cybercrime" in Sylvia Papadopoulos and Sizwe Snail (eds), *Cyberlaw @ SA III: the Law of the Internet in South Africa* (Van Schaik 2012).

[13]OlusolaMaitanmi and others, "Impact of Cyber Crimes on Nigerian Economy" (2013) 2 *The International Journal of Engineering and Science* (IJES) 45 <http://theijes.com/papers/v2-i4/part.%20(4)/H0244045051.pdf> accessed March 25, 2021.

jurists, scholars and policy commentators in Nigeria.[14] These definitions failed to differentiate computer and computer system as it is superfluous and need to be more explicit in defining the concept of cybercrime. A person may be involved in cybercrime though is not a criminal, for instance, a person who engages in cyber pornography is not a criminal hence, the definition seems narrow.

Yazdanifard, Oyegoke and Seyedi[15] defined "cybercrime" as any type of intentional criminal scheme that is a computer or/and internet-mediated. However, whilst such a description describes a wide spectrum of cybercrime, it fails to account for the dual model of criminal schemes within cyberspace. Ogwezzy[16] elaborated that the term "cybercrime" implies offences committed through the use of the computer in contrast to "computer crime" which refers to offences against the computer and data or program therein. Thus, whilst the computer and its contents are the primary targets in computer crimes, the meaning of cyber-crime is wrapped around the use of a computer or/and the Internet to commit age-old crimes. These definitions are inclusive and broad in defining the concept of cybercrime.

Furnell in his paper[17] considered the difficulty associated with categorising 'cybercrime', and identified that a harmonised nomenclature would be beneficial to individuals and organisations concerned with combating the problem, as well as to those concerned with reporting the issue to the general public. Other interchangeable terms are also often used, such as 'virtual crime', 'net-crime', 'hi-tech crime' or 'computer crime.'[18] The lack of clarity can be confusing and disconcerting and has led to a tendency, amongst some, to label any offence that involves a computer or part thereof as a cybercrime.

---

[14]ChinwezeUzochukwu, Onyejegbu Dominic Chukwuemeka and Friday Raphael Egbegi, "An Exploratory Study of Cybercrime in the Contemporary Nigeria Value System" (2019) 0 *European Journal of Social Sciences Studies*<https://oapub.org/soc/index.php/EJSSS/article/view/565> accessed March 25, 2021; MO Ifukor, "Cybercrime: A Challenge to Information and Communication Technology (ICT)" (2006) 8 *Communicate: Journal of Library and Information Science* 38.; AO Obuh and IS Babatope, "Cybercrime Regulation: The Nigerian Situation" in Esharenana E Adomi (ed), *Frameworks for ICT Policy: Government, Social and Legal Issues* (IGI Global 2010) pp. 98 – 112;

[15]RashadYazdanifard, Tele Oyegoke and Arash Pour Seyedi, "Cyber-Crimes: Challenges of the Millennium Age" in D Zheng (ed), *Advances in Electrical Engineering and Electrical Machines. Lecture Notes in Electrical Engineering, Vol 134* (Springer 2011).

[16] Michael ChukwujinduOgwezzy, "Cyber Crime and the Proliferation of Yahoo Addicts in Nigeria" (2012) 1 AGORA *International Journal of Juridical Sciences* 86, 91

[17] Steven Furnell, "Categorising Cybercrime and Cybercriminals: The Problem and Potential Approaches" (2001) 1 Journal of Information Warfare 35 <https://www.jstor.org/stable/26486092> accessed March 23, 2021.

[18]*Ibid*. p 21

The European Commission relies on three categories to define cybercrime. According to the EU Cyber Security Strategy of 2013[19]:

> Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (such as fraud, forgery, and identity theft), content-related offences (such as online distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (such as attacks against information systems, denial of service and malware).[20]

The limited use of a strict definition in national legislation is an issue pointed out in the UNODC's report titled "Comprehensive Study on Cybercrime – 2013". The report noted that the majority of these nations do not appear to be concerned with having a strict definition. Rather, legislation more commonly referred to computer crimes, electronic communications, information technologies, or high-tech crime.

To illustrate the *status quo* described by the UNODC and how the term differs across jurisdictions, the National Cyber Security Strategies of seven nations[21] were examined to compare and contrast different definitions or descriptions of 'cybercrime'. This is not an exhaustive list, but an illustration of the differing non-legislative definitions or descriptions used across jurisdictions. Of these seven strategies, three (including Nigeria) do not define or describe the term but do address the issue of cybercrime. In the Australian Cyber Security and Policy document, "cybercrime" refers to crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software[22]. This definition is narrow as it fails to include computer space or network. It also includes crimes where computers are part of an offence, such as online fraud[23]. The Danish position is somewhat similar where the policy

---

[19] European Commission (EC), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (European Commission 2013) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf>. Accessed 25 March, 2021.

[20] *Ibid*. p 3

[21] Australia, Denmark, Ireland, Netherlands, New Zealand, Nigeria and United Kingdom

[22] Australian Government, *Australia's Cyber Security Strategy 2020* (Commonwealth of Australia 2020) p. 10

[23] *Ibid*. p 12

document notes that Cybercrime refers to perpetrators that use cyber-attacks to commit financially motivated crimes[24]. Cybercrime cannot be referred to as perpetrators but the act of perpetrating, hence the definition seems faulty. In the Irish National Cyber Security Strategy 2019-2024, cybercrime comprises traditional offences (e.g. fraud, forgery and identity theft); content-related offences (e.g. online distribution of child sexual abuse material, hate speech or incitement to commit acts of terrorism); and offences unique to computers and information systems (e.g. attacks against such systems, the spread of malware, hacking to steal sensitive, personal or industry data and denial of service attacks to cause financial and/or reputational damage)[25]. This definition is comprehensive and over-inclusive as it examines the basic elements of cyber offences which involve computer and the internet. Electronic devices are also used to sell and transfer all sorts of illicit goods and services, from illicit drugs to online child sexual abuse and exploitation materials to lists of stolen credit card numbers[26]. The Nigerian Cyber security Policy does not also define cybercrimes but notes the prevalent and emerging crimes in the Nigerian cyberspace that needs tackling such as phishing, business email comprises (BEC), ransom ware and identity thefts[27].

The term "cybercrime", under the Netherland's National Cyber Security Agenda, covers a broad range of criminal actions, from classic crimes in digital form to new forms of crime. This involves, for instance, hacking computers to transfer money to criminal bank accounts or turning on cameras and microphones undetected to be able to spy on people in their surroundings[28]. On the other hand, the New Zealand position is that cybercrimes are crimes that are committed through the use of computer systems, and are directed at computer systems. Examples, include producing malicious software, denial of service attacks, and phishing. Thus, cyber-enabled crimes are crimes that are assisted, facilitated or escalated in scale by the use of technology. Examples are cyber-enabled fraud and the online distribution of child exploitation material[29]. The United Kingdom

[24] Danish Government, *Danish Cyber and Information Security Strategy 2018-2021* (Ministry of Finance 2018) p. 6 <https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf>.Accessed March 25, 2021.

[25] Government of Ireland, *National Cyber Security Strategy 2019-2024* (Government of Ireland 2019) <https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf>Accessed March 15, 2021.

[26] *Ibid.*

[27] Federal Government of Nigeria, *National Cybersecurity Policy and Strategy* (Federal Government of Nigeria 2021). p. 4

[28] Netherlands Government, *National Cyber Security Agenda - a Cyber Secure Netherlands* (Ministry of Justice and Security 2018) p. 35 <https://www.cyberwiser.eu/sites/default/files/NL_NCSS_2018_en%20%282%29.pdf> Accessed March 24, 2021.

[29] New Zealand Government, *New Zealand's Cyber Security Strategy 2019* (National Security Group (NSG) 2019) p. 16 <https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf>. Accessed March 24, 2021.

distinguishes the various nature of cybercrimes into 'cyber-dependent crimes' and 'cyber-enabled crimes'. Cyber-dependent crimes are crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity). Conversely, Cyber-enabled crimes - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT such as cyber-enabled fraud and data theft[30].

It is surprising that the Nigerian Cybercrime Act, the Council of Europe Cybercrime Convention, and the African Union Convention, contain no definition of cybercrime. The fact that before the adoption of the African Union Convention and subsequent enactment of the Nigerian Act, there had been many conflicting and diverse connotations of what acts or conducts amounted to cybercrime, it would have been expected that both legislation includes a workable definition of cybercrime. Maybe, an issue that has made the global definition of cybercrime so difficult has been the constantly changing and evolving scope of computer-related crimes; more so, as definitions of cybercrime continue to evolve.[31] The continuous expanding nature of technology has made offenders become more sophisticated in their criminality and broaden their acts towards new variations in computer crimes outside the confines of the jurisdictional statutory definition of cybercrime, and thereby making it more difficult for the procedural enforcement of cybercrime laws.[32]

Through the various definitions analysed, it is apparent that as it relates to cybercrime, the computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime.[33] In all cybercrimes, computers and the Internet are used as tools. Even if what is in question is an attack where computers or networks, or information is targeted, the necessary tools are still computers and the Internet, without which the offence may fall into the traditional offences, and cannot be classified as cybercrimes. However, technological involvement is a necessary but not

---

[30] HM Government, *National Cyber Security Strategy 2016 to 2021* (Cabinet Office 2016) p. 17 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>. Accessed March 13, 2021.

[31] Sarah Gordon and Richard Ford, n. 27.

[32] YasinAlsan, "Global Nature of Computer Crimes and the Convention on Cybercrime" (2006) 3 *Ankara Law Review* 129.

[33] Sarah Gordon and Richard Ford, n. 27.

sufficient condition. Illegally assembling computers with market traded computer parts can hardly be a cybercrime[34]. Yet, illegally manufacturing computer chips can be[35]. If traditional forces and technological means are combined in a certain offence, both cybercrime and the traditional offence can run together. For example, a bank employee may be abducted and forced to reveal IDs and passwords. The combined use of these means is not rare in practice.

Although there is still no universally accepted definition for cybercrime, those jurisdictions that have defined this term seem to have the same goal of criminalising trans-border cybercriminal activities perpetuated by or directed at data, computers, and/or computer networks through the internet. Also, given the saturation of Internet-connected technologies in everyday life, much of all crime exists on a technological spectrum. Several legal and ICT commentators have since abandoned their initial definitional quests; as the distinctions they make have become increasingly blurred. Furthermore, in the investigations and prosecutions of cybercrimes or related offences, it has been noted that many offenders may engage in a range of cyber-enabled, cyber-dependent and offline offences to achieve their goals. This can complicate definitions and add to the problems of assessing cybercrime levels[36]. Again, Furnell, noted that it may be more important to make sense of the actual threat posed, the harm it causes and how to prevent it, than focus on situating cybercrimes into particular categories[37]. He suggested that definitional work was hampered by the rapid speed of threat emergence mentioned above, as well as the broad range of actors.

Nonetheless, a working definition is offered by Thomas and Loader, who conceptualized cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"[38].

The specificity of cybercrime is therefore held to reside in the newly instituted interactional environment in which it takes place, namely the "virtual space" or "cyberspace" generated by the interconnection of computers into a worldwide network of information exchange, primarily the

[34]PerewareAghwotuTiemo and Digitemie-BatuboBeleudaara Nelly, "Efforts in Combating Cyber Crime and Criminality in Nigeria" (2016) 6 *Information and Knowledge Management* 23.

[35] E RutgerLeukfeldt, Anita Lavorgna and Edward R Kleemans, "Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime" (2016) 23 *European Journal on Criminal Policy and Research* 287.

[36]RashadYazdanifard, Tele Oyegoke and Arash Pour Seyedi, n. 19.

[37] Steven Furnell, "Cybercrime: Vandalizing the Information Society," *2003 International Conference on Web Engineering* (2003).

[38] Douglas Thomas and Brian Loader, Cybercrime: Security and Surveillance in the Information Age (Routledge 2000) p. 19

Internet. Within this definition, it is possible to further classify cybercrime along several different lines.

Having examined and analysed the various definitions and nature of cybercrime as enunciated by different authors, international agencies and some jurisdiction, it is therefore important to state that this paper is of the opinion that cybercrime are offences committed using the internet and the computer system for nefarious activities which have negative impact on the individuals, economy and society as large.

Scope of Cyber Crime

Cybercrime can generally be divided into two broad categories – crimes that are facilitated by computers or the Internet, and crimes against computers or computer system.[39] Cyber-crime is an extension of traditional crime but it takes place in cyberspace[40] – the non-physical environment created by computer systems. By utilizing globally connected phone systems and the world's largest computer network, the Internet, cyber-criminals can reach out from just about anywhere in the world to just about any computer system, as long as they have access to a communications link.[41]The ability of worldwide access has resulted in a territory-less dimension of cybercrime. Cybercrime, therefore, has an international aspect that creates many difficulties for nations that may wish to halt it or simply mitigate its effects. Moreover, cyber-crime is generally understood as the use of a computer-based means to commit an illegal act. One typical definition describes cyber-crime as any crime that is facilitated or committed using a computer, network, or hardware device.[42]As cybercrime is not bound by physical borders the criminal can found anywhere around the world – which itself has made cybercrime a universal natured crime.

The criminal activities which constitute cybercrime are not defined and there is no exhaustive list providing all sets of cybercrime. There are several definitions of cybercrime which have separate specification of crime categorizing as cybercrime. The scope of criminal activities and their social consequences can be summarized by a typology of computer-related crime that comprises of two

[39] Gerald Ferrera and others, *CyberLaw: Text and Cases* (3rd edn., South-Western College/West 2011) p. 402.
[40]E Gabrys, "The International Dimensions of Cyber-Crime, Part I" (2002) 11 *Information Systems Security* 21, 23
[41]*Ibid.*
[42] Anita Lavorgna, "Organised Crime Goes Online: Realities and Challenges" (2015) 18 *Journal of Money Laundering Control* 153.

sets of crimes,[43] i.e., conventional crimes, in which computers are instrumental to the offences, such as online attacks on computer networks, destruction of databases etc. and online criminal cases in which evidence exists in digital forms, such as cyber-vandalism and terrorism, insertion of viruses, worms, defamation, extortion, etc.

Similarly, McCusker has identified many offences in three sets as cybercrime threats[44], i.e., offences against the confidentiality, integrity and availability of computer data and systems (via activities such as hacking, deception, interception and espionage), computer-related 'traditional' crimes (fraud and forgery), content-related computer offences (such as website defacement and dissemination of false information) and offences relating to the infringement of copyright and related rights (such as the unauthorized reproduction and use of programs and databases).

The different actions that may amount to crime have been broadly classified into three categories. Firstly, cybercrimes where the computer is used as a target which includes offences such as sabotage of computer systems or computer networks or operating system and program, theft of data or information or intellectual property such as software or marketing information, blackmailing based on information gained from computerized files such as personal history, sexual preferences, financial data, etc. and Illegal access. Secondly, cybercrimes, where the computer is an instrument facilitating the crime, includes offences such as software piracy, counterfeiting, copyright violation of computer programs, theft of technological equipment and illegal sale of the duplicate CD. Thirdly, cybercrimes where the computer is incidental to other crimes which include those crimes in which computer is not essential for the crime to occur, but computerization does help in the incidence of crime by the processing of huge amount of information and makes the crime more difficult to be traced and identified – example money laundering, unlawful banking transactions

Thus, from the discussion above, any activity that uses a computer as an instrumentality, target or a means for perpetrating a further crime, falls within the ambit of cybercrime. As postulated above, definitions and nature of cybercrime have been focused on the functional part rather than a universally accepted legal definition. The *sine qua non* for cybercrime is that there should be an involvement of virtual cyber medium (computer) at any stage of crime. From the scholars' view

[43]RodericBroadhurst, "Developments in the Global Law Enforcement of Cybercrime" (2006) 29 *Policing: AnInternational Journal of Police Strategies and Management* 408.

[44] Rob McCusker, "Transnational Organised Cyber Crime: Distinguishing Threat from Reality" (2007) 46 *Crime, Law and Social Change* 257.

and legal propositions, there are some peculiar features of cybercrime[45], viz., (i) cybercrime is a global phenomenon that does not have any territorial barriers or jurisdictional restrictions, there is non-existence of any physical evidence, (ii) evidence of cybercrime is in a digital format identified only by trained and skilled person, (iii) perpetrator of cybercrime largely be technocrats; and (iv) cybercrime is new approach identified by perpetrator such as electronic vandalism, transnational crime, electronic money laundering, counterfeiting, etc. which includes computer network attack as well as an electronic approach of committing traditional crimes and there is non-requirement of disclosure of identity – can manage anonymity.

To overcome cybercrime, Wall purports that one should consider how the use of ICT transforms a crime, rather than the act itself[46]. To do this, he suggests the use of an elimination test, in which one thinks about what would happen if the use of ICT were removed from the offence. From this approach laid out by Wall, Parodi noted that three different types of opportunity emerge[47]. The first are behaviours often called 'cybercrimes' that are "traditional crimes" in which a computer has been used – exemplified by the use of ICT in the commission of a crime such as fraud. The second is "hybrid cybercrimes" which are traditional crimes for which network technology has created entirely new global opportunities – exemplified through global frauds. The third is "true cybercrimes" which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace – exemplified through spam, phishing and other forms of social engineering.

Similarly, Grabosky[48] also breaks cybercrime into three forms. These three forms are (1) conventional crimes committed with computers, such as digital child pornography, piracy, or intellectual property theft, and forgery; (2) attacks on computer networks; and (3) conventional criminal cases such as drug trafficking, in which evidence exists in digital form.

Although slightly different, these categorisations are important not only in the context of providing clarity about the role of ICT in criminality, but also concerning response, and especially in the context of legislative applicability. The first of Wall's two categories stem from traditional crimes, which he suggests are likely to be the subject of existing laws. Any legal problems enforcing such

[45]VishwanathParanjape, *Cyber Crimes & Law* (Central Law Agency 2010) pp. 24-26.
[46]*Ibid*. p. 26
[47]FilippoParodi, "The Concept of Cybercrime and Online Threats Analysis" (2013) 2 *International Journal of Information Security and Cybercrime* 59.
[48] Peter Grabosky, "The Global Dimension of Cybercrime" (2004) 6 *Global Crime* 146.

laws when applied to crimes that involve the use of ICT tend to relate more to legal procedures rather than substantive law, he argues. However, Wall noted that it was the third category - those crimes that are solely the product of ICT - where problems can exist in regard to responding or managing them. It is this perspective that will be explored further in this research.

Others prefer two categories. Gordon and Ford[49] argue cybercrime can be distinguished by how a computer or ICT is used in the commission of the offence. For example, category one includes crimes that involve computers or ICT as the primary factor, such as malware, in contrast to category two, which involves humans as the primary factor, such as online grooming. This distinction is somewhat similar to that made in the United Kingdom's National Cyber Security Strategy where the term is broken down as cyber-enabled crimes and cyber-dependent crimes[50]. This distinction is often said to be based on new and old crimes.

Unlike Wall, Arora in her paper[51] posited that cybercrimes can be categorized into two forms: (a) Type I and Type II. To him, Type I cybercrime is generally a single event from the perspective of the victim, while Type II cybercrimes refer to ongoing series of events, involving repeated interactions with the target such as computer-related frauds, credit card frauds etc. Generally, to him, cybercrimes are criminal activities perpetuated using cyberspace as a communication medium. Cybercrime is not only limited to the cyberspace as offences committed on the computer system could also be refer to as cybercrime, hence the author's scope of cybercrime seems narrow to the cyberspace.

Ibrahim[52] argued that the grouping of cybercrimes according to criminals' motivations was important in the definition and delineation of the offences or activities of cybercrimes since it was perpetuated often on a global scale[53]. He noted that the existing traffic between cyber-enabled and cyber-dependent categories as expounded by Wall clearly illustrated the complexity of cybercrime and how one criminal act can impact multiple nations and involve various networks of actors

[49] Sarah Gordon and Richard Ford, "On the Definition and Classification of Cybercrime" (2006) 2 *Journal in Computer Virology* 13.

[50] Matthew Hull, Thaddeus Eze and Lee Speakman, "Policing the Cyber Threat: Exploring the Threat from Cyber Crime and the Ability of Local Law Enforcement to Respond," *2018 European Intelligence and Security Informatics Conference (EISIC)* (2018).

[51] BhavnaArora, "Exploring and Analyzing Internet Crimes and Their Behaviours" (2016) 8 *Perspectives in Science* 540 <https://www.sciencedirect.com/science/article/pii/S2213020916301537> accessed March 23, 2021.

[52] Suleman Ibrahim, "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals" (2016) 47 *International Journal of Law, Crime and Justice* 44.

[53] *Ibid*. p. 45

simultaneously. To him, closely related to cyber-enabled and cyber-dependent categories are the 'techno-centric (type I) and people-centric (type II) subsets'. Type 1 (techno-centric) crimes such as e-commerce fraud, cyber-vandalism, data manipulations through hacking, phishing, from Type II (people-centric) crimes such as cyber fraud, cyber bullying and cyber-stalking. Therefore, he opined that cybercrime can be conceptualised simply as the use of computer/Internet to commit fraud because "Nigerian cybercriminals to date, have been consistently implicated in money-oriented rather than psychosocial and geopolitical cybercrimes"[54]. It is important to note that hacking involves the human being, therefore, it cannot be categorized as techno centric same with phishing and impersonation. The distinction is unnecessary.

According to Hull, Eze and Speakman[55], cyber-dependent crimes are viewed in the United Kingdom as new crimes, which could not exist without ICT, often described as 'true cybercrimes'. In legal parlance, ICT is required to commit the *actus reus*[56] of the crime. While cyber-enabled crime, often said to be traditional crimes, are enhanced or scaled through the use of ICT. For example, online fraud where fraud can be conducted without the use of ICT, but its scale and reach can be increased through the use of ICT. According to McGuire & Dowling[57], two of the most widely published instances of cyber-enabled crime relate to fraud and theft[58].

Having the various methods or ways of categorizing by different authors, this paper is of the view that cybercrime should be categorized in terms of the offences committed through the cyberspace. The nature and scope of the offence should be the fulcrum and determinant of the categorization of cybercrime and not the intention as postulated by some authors.

Conclusion

It is obvious that various authors have given divergent conceptual analysis of cybercrime depending on their perception and the purpose in which the term is used. However, it appears there is no uniformity and categorization of acceptable definition by authors, international bodies and some jurisdiction. The issue of nomenclature as used by different authors has further compounded

[54] *Ibid*. p. 49
[55] Matthew Hull, Thaddeus Eze and Lee Speakman, n. 28
[56] The *actusreus* consists of some act or some omission forbidden by law. The conduct of the accused must come within the forbidden action. The *actus* must be directly attributable to the accused and not to another person, unless the accused incited that other person or they shared a common purpose. The *actus* must be done voluntarily – *Idowu v. the State* (2002) 12 NWLR (Pt. 680) 48
[57] Mike McGuire and Samantha Dowling, *Cyber Crime: A Review of the Evidence* (UK Home Office 2013).
[58] *Ibid*. p. 4

the difficulty in achieving and acceptable or generally acceptable definition. Some jurisdictions adopt a workable definition in order to used same as a means of or as a weapon to create punishment to fight certain criminality in their countries. It is therefore important to conclude that the nature and scope of cyber offences should be the basis for the categorization of cybercrime and not the intention as postulated by some authors.

Recommendation

In the light of the above analysis, it is imperative to recommend thus:

1. There is need for a unified or acceptable nomenclature in describing cybercrime. It is also necessary to limits the scope of cybercrime to ensure strict categorization and avoid over inclusion.
2. There is need for countries to define cybercrime in their cybercrime laws so that it can be used as workable definition in their policy making or research.
3. The need to focus on implementing cyber security plans in addressing cybercrime cannot be overemphasized as organizations and institutions need to commit resources to educate employees and the general populace on cyber security practices to prevent unnecessary interference on information and data.
4. There is need for sensitization of the populace against the antics of cyber criminals in gaining access to the private database of individuals and institutions.