APPRAISING THE CYBERCRIMES (PROHIBITION, PREVENTION ETC.) ACT, 2015 IN THE CONTEXT OF JURISDICTION IN CYBERSPACE*

Abstract

The Nigerian Cybercrimes (Prohibition, Prevention Etc) Act 2015 is the fundamental legislation regulating activities of persons and organizations within the Nigeria's cyberspace. The Act governs detection, prevention, investigation, arrest and prosecution of computer and computer networks or internet related crimes in Nigeria. The aim of this work is to appraise the Cybercrimes (Prohibition, Prevention Etc) Act, 2015 in the context of jurisdiction in cyberspace. Its major objectives are: to make an overview of the cybercrimes Act; to determine the bases of jurisdiction in cyberspace; to appraise the issue of state's sovereignty in cyberspace; to ascertain the type of jurisdictions in cyberspace created by the cybercrimes Act 2015 and to establish the bases of cyberspace inherent in the cybercrimes under the Act. Doctrinal research methodology was adopted. It was the findings of this work that the physical and human components of cyberspace are subject to the sovereign powers of the state to prescribe, adjudicate and enforce while the software component, by virtue of its de-territorialized and trans-boundary nature may not be subject to territorial jurisdiction of the state. This work concluded that the physical and the human components of cyberspace are subject to the territorial jurisdiction of the state and that the software component is not subject to the territorial jurisdiction of the state; the bases of jurisdiction created by the cybercrimes Act 2015 in its section 50(1) are: subjective territoriality, objective territoriality, and nationality and so on. It is recommended that the software component of cyberspace be treated as fourth international space and that UN should put in motion steps to formulate an international convention or covenant on cybercrimes.

Key Words: Cybercrimes, Cyberspace, Jurisdiction, Appraising.

1. Introduction

The Black's Law Dictionary defines cybercrime to mean, 'a crime involving the use of computer such as sabotage or stealing of electronically stored data.[1] It is the use of computer or computer related tools as instruments to further illegal ends, such as committing fraud, trafficking in child pornography, intellectual property theft, stealing identity or online piracy infractions and so on. It is analogous to cyber theft. The Black's Law Dictionary defines cyber theft as 'the act of using an online computer service, such as one on the internet, to steal someone's else property or to interfere with someone's else use and enjoyment of property.[2]

Cyberspace is the worldwide network of information systems that enable computer users to communicate or access information.[3] It has also been concluded to be a world that is both everywhere and nowhere; but it is not where bodies live.[4] It is a 'bordless' world; computer-based communication cut across territorial borders, creating a new realm of human activity.[5] UNESCO defines cyberspace as

***OYEPHO, Akeuseph, LLB, LLM (RSU), Ph.D** Research Candidate (RSU), Managing Solicitor, Oyepho Oyepho & Co. 10A Deacon Iheke Street, Mgbuoba, Port Harcourt. Email: akeusephoyepho@gmail.com; Phone number: 08035761997, 08081818383.

[1] GA Garner, *Black's Law Dictionary* (11thEdition USA: Thomas Reuter 2019), 466.

[2]Ibid, 487.

[3]Ibid, 486.

[4] JP Barlow, 'A Declaration of the Independence of cyberspace, Electronic Frontiers Foundation 8th February 1996'<https://www.eff.org/cyberspace.independence> accessed 4th May, 2024.

[5] Asian – African Legal Consultive Forum (AALCO), 'International Law in Cyberspace' prepared by AALCO secretariat, 56th Annual Session of AALCO, Nairobi 1 – 5 May 2017, Doc AALCO/56/NAIROBI/2017/SD/S17, para 1.

'a worldwide virtual space, different from real space, with many sub-communities unevenly distributed using a technical environment – first of all the internet in which citizens and organizations utilize information and communication technology for their social and commercial transaction.'[6] In other word, it is a fictional place (rather than having a tangible nature) used to describe the phenomenon of electronic signals transmitting through the infrastructure of Information and Communications Technology (ICT).[7]

Cyberspace has three components: the physical component (switches, routers, servers, cables), software component (logical network), and the third component consisting of data packets and electronics–the people actually on the network (cyber-persona component).[8]In spite of its virtual nature, cyberspace as a matter of necessity needs a physical architecture.[9] Most of the components of the cyberspace in-built in it a de-territorialized and trans-boundary character. While the physical and 'cyber persona component' may fall within the territoriality and nationality principles in the jurisdiction of a state to prescribe, adjudicate and enforce; the software components– the logical interconnectivity of networks which defile territorial boundaries may be difficult to rope into the sovereign powers of a single state, thus, it posses jurisdiction problems. It is as a result of the sovereignless nature of the internet or communication networks, that the cyberspace has been recommended to be treated as the fourth international space for the purposes of ascertaining jurisdiction.[10]

This paper will give an overview of the cybercrimes (Prohibition, Prevention etc) Act, 2015, in the context of jurisdiction in cyberspace; also, state sovereignty in cyberspace and the bases of jurisdiction in cyberspace, types of jurisdictions recognized binder international law, types of international spaces and their jurisdictional implications and the need to treat cyberspace as a fourth international space will be appraised.

2. Overview of Cybercrimes (Prohibition, Prevention Etc.) Act, 2015

The Cybercrimes Act is the principal law in Nigeria governing detection, prevention, investigation, arrest and prosecution of computer and computer networks or internet related crimes in Nigeria. It deals with issues related with the internet, computing, cyberspace and associated matters.[11] The Act provides or creates effective unified and comprehensive normative and institutional structure for the prohibition, prevention, detection, arrest, prosecution and punishment of cybercrimes in Nigeria.[12] Crimes created by the Cybercrimes Act include but not limited to: Offences Against Critical National Infrastructure,[13] Unlawful Access to a Computer,[14] Operation and Usage of Unregistered Cyber case,[15] System

[6] UNESCO, 'International Governance Glossary' <https://en.unesco.org/glossaries/igg/group/1%20internet%20governance@20general> accessed 4th May, 2024.
[7] A Berkes, 'Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside its Effective Control (2019)(52) (2) Israel Law Review 201.
[8] N Tsagourias, 'The Legal States of Cyberspace' in Nicholas K Tsagourias and Russell Buchan (eds) *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015), 15.
[9] PW Franzese, 'Sovereignty in cyberspace. Can it exist'? (2009)(64) Airforce Law Review 1, 33.
[10] DC Menthe, 'Jurisdiction in cyberspace: 'The theory of International Spaces' (1998)(4)(69) *Michigan Telecommunications and Technology Law Review*, 70.
[11] J Uba, 'Cybercrimes and cyberlaws in Nigeria: All you need to know' <https://www.mondaq.com/nigeria/security> accessed 4th May, 2024.
[12] Cybercrimes (Prohibition, Prevention Etc) Act 2015, Section 1(a).
[13]Ibid, Section 5(1) and (2).
[14]Ibid, Section 6.
[15]Ibid, Section 7.

Interference,[16] Interception of Electronic Messages and Emails, Electronic money transfer,[17]tempering with critical infrastructure,[18] Willful misdirection of electronic messages[19] and so on.

The Act is a combination of eight parts which with fifty eight sections and schedules. Part one deals with object and application of the Act; it contains sections 1 and 2 of the Act. The objectives of the Act as contained in section 1(1) (a) (b) & (c) are to:

a. provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.
b. ensure the protection of critical National Infrastructure; and
c. promote cyber security and the protection of computers and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

Section 2 provides that the Act shall apply throughout the Federal Republic of Nigeria.[20] Thus, no State House of Assembly can vividly make any law on regulating cybercrime in a State. This provision reinstates the constitutional doctrine of covering the field as guaranteed by section 4(5) of the Constitution of the Federal Republic of Nigeria 1999 (as amended), which provides that:

> If any law enacted by the House of Assembly of State is inconsistent with any law validly made by the National Assembly, the law made by the National Assembly shall prevail, and that other law shall to the extent of the inconsistency be void.[21]

Part two contains Sections 3 and 4, which provides for the protection of Critical National Infrastructure and authorizes the President on recommendation of the National Security Adviser to designate and publish in the Federal Gazette certain computer system and/or traffic data vital to the country that the incapacitation or destruction of or interference with such system and assets will have a debilitating impact on security, national or economic security, national public health and safety or any combination of these matters as constituting critical information infrastructure.[22] The presidential order by the intendment of Section 3(2) will also prescribe minimum standards, guidelines, rules or procedures pertaining to the protection, preservation, general management, access to transfer and control information and data in any critical infrastructure.[23] By Section 4, it is the responsibility of the National Security Adviser upon directive contain in a presidential order to audit and inspect, any critical National information infrastructure at any State.[24]

Part three of the Act creates offences and penalties; it is a combination of Sections 5 – 36 of the Act.[25] The offences and penalties created by the Act include but not constrained to: offences against critical national information infrastructure in its Section 5(1), which attracts a punishment of ten years imprisonment on conviction without option of fine; by Sub-section (2) & (3) of Section 5,[26] where the offence committed against critical national infrastructure results in grievous bodily harm to any person, the offender shall be liable on conviction to imprisonment for a term of not more than fifteen years

[16]Ibid, Section 8.
[17]Ibid, Section 9.
[18]Ibid, Section 10.
[19]Ibid, Section 11.
[20] Cybercrimes Act, (n[12]), Section 2.
[21] Constitution of the Federal Republic of Nigeria 1999 (as amended), Section 4(5).
[22] Cybercrimes Act (n[12]), Section 3(1).
[23]Ibid, Section 3(2)(a)(b) & (c).
[24]Ibid, Section 4.
[25] Cybercrimes Act (n[12]), Sections 5 – 36.
[26]Ibid, Section 5(1) &(2).

without option of fine; and where the offence committed against critical national infrastructure results in death, the offender shall be liable on conviction for life imprisonment;[27] operation of unregistered cybercafé,[28] is an offence under Section 7, system interference,[29] is an offence under section 8, unlawful access to computer,[30] is an offence under section 6, interception to electronic message and email, electronic money transfer,[31] tempering with critical national infrastructure;[32] is an offence under section 10, willful misdirection of electronic message,[33] computer related forgery,[34] is an offence under section 13, unlawful interception,[35] computer related fraud,[36] theft of electronic devices,[37] cyber terrorism,[38] identity theft and impersonation,[39] child pornography and related offences,[40] cyber stalking,[41] cybersquatting,[42] manipulation of ATM (POS Terminals),[43] phishing, spamming and spread of computer virus[44] and so on, with punishments ranging from life imprisonment, imprisonment term and/or fines. In the proceeding sub-title, an attempt will be made to give succinct explanations of the different cybercrimes created by the Act and other laws.

Part four focuses on the responsibility of financial institutions and service providers. By Section 37(1)(a) of the Act, 'financial institution shall verify the identity of its customers carrying out electronic financial transactions by requesting customers to present documents bearing their names, address, and other related information before issuance of ATM cards, credit cards, debit cards and other related electronic devices. Financial institution shall apply the principle of know your customers in documentation of customers, preceding execution of customers transfer payment, debit and issuance orders;[45] any official or organization who fails to obtain proper identification of customers before executing customers electronic transaction whatever way, commits an offence and shall be liable on conviction to a fine of five million naira (₦5, 000,000).[46] Also, by Section 37(3) of the Act, any financial institution that makes an unauthorized debit on a customer's account shall upon written notification by the customer, provide clear legal authorization for such debits to the customer or reverse such debit within seventy two hours (72hrs). Any financial institution that fails to reverse such debit within 72 hrs, shall be guilt of an offence and liable on conviction to restitution of the debit and a fine of ₦5, 000,000.00.[47] Similarly, Section 38(1) & (2) placed on service providers a duty under the Act to keep all traffic data and subscriber information and shall keep them for a period of two years and shall upon request of relevant authority or any law enforcement agency preserve, hold, or retain any traffic

[27]Ibid, Section 5(3).
[28]Ibid, Section 7(1) (2) & (3).
[29]Ibid, Section 8.
[30]Ibid, s. 6.
[31]Ibid, Section 9.
[32]Ibid, Section 10.
[33]Ibid, Section 11.
[34]Ibid, Section 13.
[35]Ibid, Section 12.
[36]Ibid, Section 14.
[37]Ibid, Section 15.
[38]Ibid, Section 18(1) & (2).
[39]Ibid, Section 22.
[40]Ibid, (n^1), Section 23.
[41]Ibid, Section 24.
[42]Ibid, Section 25.
[43]Ibid, Section 30.
[44]Ibid, Section 32.
[45] Cybercrimes Act (n^{12}), Section 37(1)(b).
[46]Ibid, Section 37(2).
[47]Ibid, Section 37(3).

data, subscriber information, non-content information, content data release any information required.[48] Service providers are mandated by the Act to release any information required by law enforcement agency through its authorized officer[49] but the service provider as well as the law enforcement agency performing this duty must have regard to the individual's right to privacy under the Constitution.[50] By the meaning of Section 38(6) of the Act, if a service provider or an officer of a law enforcement agency contravenes in the exercise of the duty placed on him by this section, he commits an offence and shall be liable on conviction to imprisonment for a term not more than a 3 years or fine of not more than ₦7, 000,000.00 or both the fine and imprisonment.[51] Generally, by Section 40(2) of the Act, service providers are under a duty upon request for any law enforcement agency to provide assistance towards:

i) the identification, apprehension, and prosecution of offenders.[52]
ii) the identification, tracking and tracing of proceeds of any offence or property, equipment or device used in the commission of any office[53] or
iii) the freezing, removal, erasure or cancellation of the offender which enables the offender to either commit the offence, hide or preserve the proceeds of an offence or any property, equipment or device used in the commission of the offence.[54]

Any service provider who fails to comply with enforcement agency in respect of rendering assistance aforestated commits an offence under Section 40(3) and shall be liable on conviction to a fine not more than ₦10, 000,000.00[55] and in addition to this punishment, each director, manager or officer of the service provider shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine not more than N10, 000,000.00 but subject to the provision of Section 20.[56]

Part five of the Act deals with Administration and Enforcement Matters; in consonance with Section 41(1), the office of the National security Adviser serves as the coordinating body for all security and enforcement agencies,[57] and among other things, provide support to all relevant security, intelligent, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria.[58] The Attorney-General of the Federation reinforces and improves Nigeria's existing legal framework regarding cybercrimes.[59] All law enforcement, security and intelligent agencies develop the institutional capacity necessary for effective implementation of the provisions of the Act and in collaboration with office of the National Security Adviser, initiate, develop or organize training programmes for officers charged with enforcement of cybercrime laws on a national or international level.[60]

The Act in its Section 42 establishes a Cybercrime Advisory Council in charge of handling issues relating to the prevention and combating of cybercrimes, cyber threat, computer-related cases and the promotion of cyber security in Nigeria.[61] The function of the Cybercrimes Advisory Council as provided in Section 43(1) of the Act, include:

[48]Ibid, Section 38(1)-(2)(a) (b) & (c).
[49] Cybercrimes Act (n[12]), Section 38(3).
[50] Constitution (n[21]), Section 37; Ibid, Section 38(5).
[51] Cybercrimes Act (n[12]), s. 38(6).
[52]Ibid, Section 40(2) (a).
[53]Ibid, Section 40 (2) (b).
[54]Ibid, Section 40 (2) (v).
[55]Ibid, Section 40 (3).
[56]Ibid, Section 40 (4).
[57]Ibid, Section 41 (1).
[58]Ibid, Section 41(1)(a).
[59]Ibid, Section 41(2).
[60]Ibid, Section 41(3).
[61]Ibid, s. 42 & 43.

a. to create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues related to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria.
b. to formulate and provide general policy guidelines for the implementation of the provisions of this Act;
c. to advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues;
d. to establish a program towards grants to institutions of higher learning to establish cyber security research centers to support the development of New cyber security defences, techniques and processes in the real-world environment; and
e. to promote graduate traineeship in cyber security and computer and Network Security Research and Development.

The Act also in Section 44 creates a National Cyber Security Fund for funding the activities of the bodies and agencies charged with the responsibility of combating cyber related misbehavior.[62]

Part six of the Act deals with issues related and connected with arrest, search seizure and prosecution of cybercrimes. The powers to arrest offenders under Section 45 of the Act is vested on law enforcement officer(s) and they may exercise this power by applying *ex-parte* to a judge in chambers for issuance of a warrant for the purpose of obtaining electronic evidence related to crime investigation;[63] the judge upon being satisfied that the warrant is sought to prevent the commission of a cybercrime or for the purpose of preventing a cybercrime, cyber security breaches, computer related offences, or obtaining evidence or there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation or the person named in the warrant as preparing to commit a cybercrime,[64] issue warrant authorizing a law enforcement office to enter and search premises, where a cybercrime is being committed.[65] Section 46 of the Act makes it an offence to obstruct a law enforcement officer, in the performance of this duty under the Act. By Section 47 relevant law enforcement agencies have power to prosecute offences created by the Act but subject to the powers of the Attorney-General.[66]

Part seven of the Act covers issues of Jurisdiction and international cooperation on cybercrimes prevention and prosecution. Section 50 empowers the Federal High Court located at any part of Nigeria regardless of the location where the offence is committed with jurisdiction to try cybercrimes in Nigeria or try the matter if committed in a slip or aircraft registered in Nigeria or by a citizen or resident in Nigeria; if the person's conduct would also constitute an offence under a law of the country where the offence was committed[67] or outside Nigeria where:

i) the victim of the offence is a citizen or resident in Nigeria.
ii) The alleged offender in Nigeria and not extradited to any other country for prosecution.[68]

Offences under the Act shall be extraditable under the Extradition Act Cap E25 LFN. 2004.[69]

[62]Ibid, Section 44.
[63]Ibid, Section 45.
[64]Ibid, Section 45(3)(a) (b) (c) & (d).
[65]Ibid, Section 45(2)(a).
[66]Ibid, Section 47.
[67]Ibid, Section 50(1) (a) – (c).
[68]Ibid, Section 50(1)(d)(i) – (iii).
[69]Ibid, Section 51.

Interlocutory application for stay of execution in respect of criminal matter highlighted under the Act shall not be obtained but subject to the provisions of the Constitution.[70] Further issues on jurisdiction will be properly examined in course of this work. The final part of the Act handles miscellaneous issues ranging from the power granted to the Attorney General to make Orders, Rules, Guidelines, Regulations for efficient implementation of provisions of the Act by the way of delegated legislation.[71] Section 58 deals with interpretation or definition of relevant words, phrases and concept.[72]

3. State Sovereignty in Cyberspace

As a result of its non-physical nature, on the face of it, cyberspace hardly fits within the international principles of public international law such as sovereignty or territorial integrity,[73] also contained in the United Nations Charter.[74] A considerable number of Liberal scholars has expressed that cyberspace should not be regulated and subjected to state sovereignty, owning to its de-territorialized and transboundry character.[75] This argument on whether or not the cyberspace should be regulated has essentially waned and is largely a historical milestone as noted by the International Law Commission (ILC).[76] Currently, it is widely accepted by states and international law scholars that state sovereignty is applicable to cyberspace, as the number of international treaties governing cyberspace has increased.[77]

The regulation of de-territorialized telecommunication activities is not a new area to international law. From the time of invention of wireless telegraphy, states, decided to exercise their sovereignty over radiographic communications in their countries.[78] Writers in the interwar period generally expressed that states control was necessary to regulate the international use of telecommunication techniques, and that a state incurs international liability for violating the prohibition on interference in the international

[70]Ibid, Section 50(4).
[71]Ibid, Section 50.
[72]Ibid, Section 58.
[73] Inter-American Judicial Committee, 'Annual Report of the Inter-American Judicial Committee to the General Assembly, OEA/Ser.Q/V134, CJI/doc.145/03, 29 August 2003, 164.
[74] Charter of the United Nations 1945, art 2(1) 8(4).
[75] DR Johnson and D G Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996)(48) *Stanford Law Review, 1367;* F Easter Brook, 'Cyberspace and the Law of the Horse' (1996) *University of Cambridge Legal Forum207*; A Segura-Serrano, 'Internet Regulation and the Role of International Law' (2006)(10) Max Planck United Nations *Yearbook of International Law* 191, 193 – 197.
[76] International Law Commission, 'Report of the ILC on the work of its 58th session (1 May – 9 June and 3 July – 11 August 2006), UN DocA/CN4/SEA.A/2006/Add.1 (part 2), 2006(11) *Yearbook of International Law Commission* 218, para 5.
[77] Budapest Convention on Cybercrimes 2001; Additional Protocol to the Budapest Convention on Cybercrime, concerning the Criminalization of Acts of Racist and Xenophobic Nature Committed through Computer System 2003; second additional protocol to the convention (Budapest convention) on Cybercrime on Enhanced Cooperation and disclosure of Electronic Evidence 2011; United Nations Convention on the use of Electronic Communications in International Contract 2005; League of Arab States, Arab Convention on Combating Information Technology Offences 2010, African Union Convention on Cyber security and personal Data protection 2014.
[78] International Radiotelegraph Convention 1912; art 1; International Convention concerning the use of Broadcasting in the cause of Peace 1936, art 1.

affairs of other state by propaganda hostile to the other states through radio.[79] To the extent that cyberspace is also a wireless from of telecommunication, the same principles apply.[80]

The application of the principle of state sovereignty in cyberspace has its main rationale in the supreme authority of the state to regulate any cyber infrastructure located within its territory,[81] even though it may exercise its sovereign prerogatives outsides the territory.[82] The physical layer or component of cyberspace is therefore subject to the sovereignty of the territorial state – whereas the vertical domain of cyberspace does not fall within the sovereignty of specific state.[83]

State sovereignty is synonymous to state jurisdiction: the later notion refers to the state's lawful power to act, or its power to decide whether and, if so, how to act, whether by legislative, executive or judicial means.[84] Put differently, it is the competence of state to regulate persons, objects and conducts under its domestic law, within the limits set by international law.[85] The term jurisdiction expresses the limits imposed under international law on the ability of a state to exercise prescriptive (or legislatives) and enforcement jurisdiction – that is, the circumstances in which the state is entitled to exercise its legal authority.[86] No state can perform enforcement functions in the territory of another state without the consent of the latter state. This rule can be derived from the territorial integrity and independence of states as enshrined in Article 2(4) of the United Nations Charter.[87] This implies that as long as the state is recognized by the international community as a sovereign of the area, it has jurisdiction over it; jurisdiction under general international law is basically territorial. That is the state enjoys full prescriptive, adjudicatory and enforcement jurisdiction over persons and objects situate in its internationally recognized territory, as well as activity occurring there.[88]

4. Bases of State's Jurisdiction in Cyberspace

The International Group of Experts that elaborated the Tallin Manual 2.0 foresaw three major bases on which the state may exercise jurisdiction over cyber activities related to its territory.[89] Rule 9 of the manual allows the state to exercise jurisdiction over 'cyber infrastructure and persons engaged in cyber activities on its territory'; 'cyber activities originating in, or completed on, its territory'; and 'cyber activities having a substantial effect in its territory'.[90] The Manual is intended to be an objective

[79] VV Dyke, 'The Responsibility of States for International propaganda (1940)(34) *American Journal of International Law* 58, 58 – 59; H Lauterpacht, Revolutionary propoganda' (1927)(13) Transaction Grotius Society 143, 162; W Frenchman, 'The Growth of State Control Over the Individual, and its effect upon the Rules of International State Responsibility' (1938)(19) British year book of International Law 118, 146 – 147.

[80] M N Schmitt (ed), *Tallin Manual 2.0 on International Law Applicable in cyber operation* (2nd edn: Cambridge University press) 20.

[81] *Ibid*, 11 para 1.

[82] *Ibid*, 60 – 71 (Rules 10 – 11).

[83] Tsagoureas (n[8]), 21, 27.

[84] B H Oxman, 'Jurisdiction of States (2007) *Max Planck Encyclopedia of public International Law* 1.

[85] Schmitt (n[80]), 51.

[86] O De Schutter and Others, 'Commentary to the Maastricht principles on Extraterritorial obligations of states in the area of Economic, Social and Cultural Rights (2012)(34) *Human Rights Quarterly* 1084, 1002 para 3. R Wilde, 'The extraterritorial Application of Human Rights Law on Civil and Political Rights' in Scott Sheeran and Nigal Rodley (eds) *Routledge Handbook of International Human Rights Law* (Routledge 2013) 640.

[87] Charter of the United Nations (n[74]), art 2(4); SS Lotus (France v Turkey), (1972) PCIJ Rep (Ser. A No.10) 18 – 19; Island of Palmas case (United States v Nethelands) (1928) Reports of International Arbitral Awards (RIAA), Vol. 11, 829, 839.

[88] Schmitt (n[80]), 52.

[89] Berkes (n[7]), 209.

[90] Schmitt (n[80]), SS (Rule 9).

restatement of the *lex lata;*[91] the relevant rule on territorial jurisdiction reflects the existing international law as accepted by states. Below are the three bases on which states may exercise jurisdiction over cyber activities related to their territory:

i) The physical presence of a person(s) or object(s) in its territory: the physical presence of a person or an object in the territory of a state provides adequate basis for the exercise of jurisdiction by that state. In this regard, in the SS lotus case, that is, France v Turkey,[92]wherein a place assimilated to Turkish territory, was resolved that the application of Turkish criminal law cannot be challenged, even in regard to offences committed there by aliens. Since information and communication technologies require some physical infrastructure, states have jurisdiction over those objects and persons engaged in cyber activities in their national territory. For example, it is recognized that states may exercise regulatory authority over the telecommunications or internet service providers that physically control the data in the territory of the state.[93]

ii) Cyber Activities Initiated and Completed in the State's Territory: This is in consonance with the principle of international law that has been recognized since the *Lotus* judgment, namely the subjectivity principle (activity originating in the state's territory) and objectivity principle (which has to do with activity completed in the state's territory) of territorial jurisdiction.[94] In cyberspace, the principle is also recognized as a basis for jurisdiction by conventions governing cybercrimes.[95]

While online activities might cross over the jurisdiction of many states, it might be difficult to determine where a cyber-activity commenced and ended. Therefore, the current tendency by state practice is to interpret territorial jurisdiction broadly, where any substantial connection between the cyber activity and state territory might serve as a sufficient basis for jurisdiction.[96]

The effects of the cyber activity on the state's territory: The third basis of jurisdiction proposed by the Tallin Manual relies on the 'effects doctrine', a jurisdictional link accepted to reflect customary international law.[97] Where an activity does not emanate from or end in the state's territory but has effect therein, the state has jurisdiction.[98] While certain domestic courts have applied the effects doctrine to cyberspace,[99] some scholars contest its applicability as it may lead to assertions of jurisdiction in virtually every state by virtue of the accessibility of the websites in all countries.[100] The majority doctrine and the international group of experts accept its applicability to cyberspace if states uses it

[91]Ibid, 2 – 3.
[92] Lotus case (n[87]), 23.
[93] United Nation General Assembly, '*Report of the special rapporteur on the promotion and protection of Human Rights and Fundamental Freedoms while countering terrorism* (23 September, 2024), UN DOC.A 169/397, para 41.
[94] Lotus case (n[87]), 23.
[95] Budapest convention (n[77]), art 22(1)(a); Arab Convention on Combating Information Technology Offences (n[77]), art 30(1)(a).
[96] Schmitt (n[80]), 57; Inter-American Commission on Human Rights (IACHR), 'Report of the special rapporteur for freedom of expression 2013, OEA/Ser.L/V/11.149, Doc.50, 496 – 497, para 66.
[97] Schmitt (n80), 56 para 5.
[98] Berkes (n[7]), 210, para 3.
[99]*LICRA and UEJF v Yahoo: Inc and Yahoo France* (2000), No. RG:00/0538 (France); *Dow Jones and Company Inc. v Gutnick* (2002) HCA 56, paras 44, 184, 198 – 199 (High Court of Australia); *people v world interactive gaming corp.* (1999) 714 NYS 2d 844, 860, paras 9 – 10.
[100] T Schmitt, 'Carving up the internet: Jurisdiction, Legal orders and the private/public international law interface' (2008)(19) *European Journal of International Law* 799, 811 – 816; M A Geist, "is there a there there – Towards greater certainty for internet jurisdiction' (2001)(16) Berkley Technology Law Journal 1345, 1349.

reasonably, setting a higher threshold of a genuine link between the state and the cyber activity than is applied in the offline world.[101]

5. Type of Jurisdictions under International Law

There are basically three types of jurisdiction recognized under international law. They are:

1. jurisdiction to prescribe;
2. the jurisdiction to enforce;
3. jurisdiction to adjudicate.[102]

The jurisdiction to prescribe is the right of a state to make its own laws applicable to the activities, relations, the status of persons, or the interest of things.[103] Enforcement jurisdiction implies the right of a state to enforce its own laws. Enforcement jurisdiction is restricted by territorial facts.[104] For instance, if a man steals a vehicle in Nigeria and manages to escape to Cotonou in the Republic of Benin, the Nigerian courts have jurisdiction to try him, but they cannot enforce it, by sending officers to Cotonou to arrest him; Nigeria has to apply to the authorities in the Republic of Benin for his arrest and extradition to Nigeria, to do otherwise, for instance, by abducting the criminal, would be a breach of territorial sovereignty of the Republic of Benin.[105] Jurisdiction to adjudicate means the tribunals of a given country have the right and competence to resolve disputes in connection to persons where the country has jurisdiction to prescribe the law that is sought to be enforced. It is instructive to note that the right of a state to prescribe laws confers in it the corresponding right to adjudicate on matters affecting the laws so prescribed and to enforce the laws principally within its territorial jurisdiction; and can only exercise its jurisdiction to enforce its own laws outside its territorial jurisdiction with the aid of Extradition treaty or Cooperation Agreement with other states.

6. Bases of Jurisdiction to Prescribe under international Law

There are six generally accepted bases of jurisdiction under which a state may claim to have jurisdiction to prescribe a rule of law over an activity.[106] They include;

a. Subjective territoriality;
b. Objective territoriality;
c. Nationality;
d. Protective principle;
e. Passive Nationality and
f. Universality.

i) Subjective territoriality is the most pertinent of the six. If an activity takes place within the territorial of forum state, then the forum state has jurisdiction to prescribe a rule for that activity. Majority of criminal legislations in the world is of this type.[107]

[101] J Kulesza, *International Internet Law* (Routledge 2012) 14 – 16; Tsagaurias (n[8]), 20; Schmitt (n80), 58 para 13.
[102] DC Menthe, 'Jurisdiction in Cyberspace: Theory International Spaces (1998) (4) (1) *Michigan Telecommunications and Technology Law Review* 71; Restatement (third) of Foreign Relations Law of the United States, 1987, 401.
[103] Menthe (n[10]).
[104] KE Oraegbunam, Jurisdictional Challenges in Fighting Cybercrimes; Any Panacea from International Law? (2015) *NAUJILJ* 59.
[105]Ibid.
[106] Menthe (n[10]), 71.
[107]Ibid, 72.

ii) Objective territoriality involves where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state.[108] For instance, if a Beninese at a border community in Republic of Benin fires a gunshot at a Nigerian who resides at a community close to the border between Nigeria and Benin; while the shooting takes place in Republic of Benin, the murder which is the effect occurs in the Federal republic of Nigeria; the Federal Republic of Nigeria would have the jurisdiction to prescribe under this principle. This is sometimes called 'effects jurisdiction" and has clear implications for cyberspace.

iii) Nationality is the basis for jurisdiction where the forum state asserts the right to prescribe or make law for an action based on nationality of the actor. Under the law of the Netherland for example, a Dutch national 'is liable to prosecution in Holland for offence committed abroad, which is punishable under Netherlands Law and which is punishable under the law of the country where the offence was committed.[109]

iv) Passive Nationality is a theory of jurisdiction based on the nationality of the victim. Passive and active nationality are often invoked together to establish jurisdiction because a state has more interest in prosecuting an offence when both the offender and the victim are nationals of the state.[110] Passive nationality is rarely used for two reasons. First, it is offensive for a state to insist that foreign laws are not sufficient to protect its citizens abroad, second, the victim is not being prosecuted, a state needs to seize the actor in order to undertake a criminal prosecution.[111]

v) Protective theory or principle expresses the desire of a sovereign to punish actions committed in other places principally because it feels threatened by those actions.[112] This principle is used where the victim would be the government or sovereign itself. For instance, in *United State v Rodriguez,*[113]the defendants were charged with making false statements in migration applications while they were outside the United States.

vi) Universal Jurisdiction sometimes referred to "universal interest" jurisdiction. Historically, universal interest jurisdiction was the right of any sovereign to capture and punish pirates.[114] This form of jurisdiction has been expanded during the past century and a half to include more of *jus cogens:* slavery, genocide and hacking (air piracy).[115] It is not yet established whether universal interest jurisdiction could be extended to internet piracy, such as computer hacking and viruses.

7. Principle of the Uploader and the Downloader in Cyberspace Jurisprudence

The public relates with cyberspace in two primary ways: either putting information into cyberspace or taking information out of cyberspace.[116] Accordingly, there are basically two distinct actors in cyberspace; the uploader and the downloader.[117] Under this theory, the uploader and the downloader act like spies in the classic information drop, the uploader puts information into a location in cyberspace, and the downloader access it at a later time. Neither need be aware of the other's identity. Unlike the classic information drop, however, there need not be any specific intent to communicate to someone as all areas of the internet are accessed by hundreds of thousands of people all over the world, while others languish as in trodden paving stones on the seemingly infinite paths of cyberspace. In both civil and criminal law, most actions taken by uploaders and downloaders presents jurisdiction difficulties. A state

[108]Ibid.
[109]Ibid.
[110]Ibid.
[111]Ibid.
[112]Ibid.
[113] 1182 F Supp 479 (S. D Cal. 1960).
[114] Menthe (n[179]), 71.
[115]Ibid.
[116]Ibid, 73.
[117]Ibid.

can forbid on its own territory, the uploading and the downloading of materials, it deems harmful to its interests. A state can therefore forbid anyone from uploading either a pornography site or gambling site from its territory and can forbid anyone within its territory from downloading, that is, interacting with the pornography site or gambling site in cyberspace.

Under international law, Nigeria has the jurisdiction to prescribe law regulating the content of what is uploaded from the territory of Nigeria. Two American cases will demonstrate how this theory works. First, in the *Schooner Exchange v Mcfaddon*[118]it was held that a French war vessel was not subject to American Law, it was in American Port. Similarly, a webpage would be ascribed the nationality of its creator, and thus not subject to the law of wherever, it happened to be downloaded. Second, the Cutting case provides an example of how an uploader should be viewed in foreign jurisdiction that is offended by materials uploaded into cyberspace. Mr. Cutting published an article in the Texas which offended a Mexican citizen. When Mr. Cutting visited Mexico, he was incarcerated on criminal libel charges. The United States secretary of State instructed the U.S. Ambassador in Mexico to inform the Mexican government that, the judicial tribunals of Mexico were not competent under the rule of international law to try a citizen of the United States for an offence committed and consummated in his own country, merely because the person offended happened to be a Mexican.[119] As a general proposition, where uploading certain material is a crime, it is an offence committed in the State where the uploader is located.

8. Bases of Jurisdiction in Cyberspace under the cybercrime (Prohibition, Prevention etc.) Act, 2015

Section 50(1) of the Cybercrimes Act confers original adjudicatory jurisdiction on offences under the Act on the Federal High Court located in any part of Nigeria regardless of location.[120] The Federal High Court by the intendment of the Act can assume jurisdiction in cyber related issues on the bases of:

i. Subjective Territoriality: The court can assume jurisdiction to entertain matters concerning grievances occasioned in cyberspace, if the acts or omissions, causing the grievances occur within the territorial of Nigeria. By Section 50(1) (a) of the Act, if the cyber-offence is committed in Nigeria, the Federal High Court in Nigeria on the basis of subjective territoriality can assume jurisdiction.[121] This is particularly possible where the cyber infrastructure used in commission of the cybercrime or violation of the cyber rights is located within the territory of Nigeria. For example, Nigeria as well as its Federal High Court has jurisdiction over person(s) manning telecommunication infrastructure and telecommunication service providers and associated companies located anywhere in Nigeria.

ii. Objective Territoriality: Nigeria as well as the Federal High Courts by virtue of Section 50(1) d(i) of the Act,[122] has jurisdiction to try any cyber related matter; even when it occurs outside the territorial boundary of Nigeria but has impacted negatively on citizen(s) of Nigeria. By the wordings of Section 50(1) (d)(i), '… offences under the Act, if committed outside Nigeria, where – the victim of the offence is a citizen or resident of Nigeria'[123] the Federal High Court has jurisdiction to entertain the matter.

iii. Nationality or Residence of the offender: By Section 50(1)(c), one of the bases of jurisdiction in cyberspace under the cybercrimes (Prohibition, Prevention Etc) Act 2015 is the nationality of the

[118] II U,S, (7 Cranch) 116 (1812).
[119] United State v Mexico (1886); More, Digest of International Law, Vol. 2, 228 (Augustus K Cutting).
[120] Cybercrimes (n[12]), s. 50(c).
[121]Ibid, Section 50(1)(a).
[122]Ibid, Section 50(1)(d)(i).
[123]Ibid.

offender or where the offender is resident in Nigeria, if the resident conduct would also constitute an offence under the law of the country where the offence was committed.[124]

From the foregoing, therefore, if the offender is a nationale of Nigeria or citizen of Nigeria, the Federal High Courts in Nigeria have jurisdiction to try cyber-related crimes committed by him.

It is hereby expressed that the bases of jurisdiction in cyberspace as provided for under section 50(1) of the cybercrimes (Prohibition, Prevention Etc.) Act, 2015 are: subjective territoriality (if the cyber activity takes place within the territory of Nigeria has jurisdiction to prescribe, adjudicate and enforce), objective territoriality (if the cyber activity takes place outside the territory of the Nigeria, but the primary effect of the activity is within Nigeria, Nigeria has jurisdiction to prescribe and even adjudicate; adjudication in this case may require mutual legal assistance between Nigeria and the foreign country where the offender initiates the cyber activity from) and Nationality (if the initiator of the cyber activity that constitutes the cyber offence, is a citizen of Nigeria, the Federal High Courts in Nigeria has jurisdiction).

9. Conclusion and Recommendations

Cybercrimes (Prohibition, Prevention Etc.) Act, 2015 is the fundamental legal framework, which provides enviable normative and institutional structure for the detection, prevention, prohibition, investigation, arrest and prosecution of cybercrimes in Nigeria. It establishes the Cybercrimes Advisory Council saddles with the responsibility among 'other things to: create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and provide recommendation on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria; advise on measure to prevent and combat computer related offences, cybercrimes, threat to national cyberspace and other cyber security related issues. The Federal High Court located anywhere in Nigeria has jurisdiction to try cyber related offences in Nigeria.

The principles or bases of jurisdiction in cyberspace under the Cybercrimes (Prohibition, Prevention Etc.) Act, 2015 are: the principles of subjective territoriality, objective territoriality and nationality principle. Cyberspace has three fundamental components; they are the physical cyber infrastructure, the persons who operate the cyber infrastructure, and the internet component. The physical cyber infrastructure and the persons operating the cyber infrastructure are subject to the territorial jurisdiction of the state where they are located. The internet and the interconnection of computer networks because of their transboundry and transnational nature may not be subject to the sovereign powers of one particular state, as a particular cyber-activity may traverses may states. It is submitted that the cyberspace particularly the networks and internet component should be treated as the fourth international sovereignless space after the outer space, high seas and the Antarctica.

It is hereby recommended as follows:

1. The software and internet layer of cyberspace should be treated as fourth international sovereignless space that should be governed by principles of jurisdiction guiding international spaces.
2. The United Nations should formulate, draft and adopt a convention on cybercrimes and cyber security, creating strong normative and institutional structure for the prevention, prohibition and combating of cyber related misbehaviours globally.

[124]Ibid, Section 50(1)(c).