UNILAG LAW REVIEW

# THE INTERNATIONAL CYBERSPACE LAW DIMENSIONS OF THE NIGERIAN CYBERCRIME ACT 2015

**Musa Kalam Abdulkadir**

**VOLUME 6 NO. 1 (2023)**

# THE INTERNATIONAL CYBERSPACE LAW DIMENSIONS OF THE NIGERIAN CYBERCRIME ACT 2015

Musa Kalam Abdulkadir*

## Abstract

*Cyber law, more than any other branch of law, is more directly implicated in the international law scheme on account of the inherent transnationality of cyber activity. Crime committed by individuals in a single country often affects the entire global space. However, while activities in cyberspace are border-blind, the actors and the architecture they exploit are effectively mapped onto specific geographic locations, either as nation-states or regional blocs. This peculiar mix necessitates an equally peculiar interplay between international law and national laws if some level of regulation of cyber activity is to be achieved. Like similar national legislations the world over, the Nigerian Cybercrime Act 2015 has a potential role to play in asserting some control over the global cyberspace. This paper investigates the provisions of the Act that are relevant to global cyberspace governance and the fight against cybercrime.*

**Keywords:** Cybercrime, Cyberspace, International law, Critical information infrastructure, State responsibility, International legal cooperation.

## 1.0 INTRODUCTION

### 1.1 An International Phenomenon

Cybercrime is essentially an international phenomenon. This is because of the nature of cyberspace, where interactions involve people in one country either transacting with people in other countries or engaging in activity in one country that causes direct

* Musa Kalam Abdulkadir is a graduate of the Ahmadu Bello University, Zaria. He is currently an LL.M Cyber Law candidate at the Faculty of Law University of Lagos, Nigeria. He is a NITDA Scholar under the National Information Technology Development Fund (NITDEF). He is a practicing lawyer with over eight (8) years at the Bar. He is also an Adjunct Lecturer at the FLA Institute for Legal and Administrative Studies, Minna Niger State, and the Kaduna State Polytechnic, Kaduna State. His research interests include cyber (IT) law, Cybersecurity, Cybercrimes, Data Protection, Cloud Computing and IP Protection in the digital environment. He is reachable at mskalaam88@gmail.com or +2348067324499.

real-world effects in another country.[1] A single cybercriminal activity often affects countless numbers of victims in many different countries, irrespective of the location of the perpetrator. For example, while allegedly originating from Pyongyang in North Korea,[2] the 2017 WannaCry ransomware attack "affected victims in more than 150 countries".[3] Empirically, it has been found that "between 50 and 100 percent of cybercrime acts encountered by the police involved a transnational element".[4] Consequently, the international community represented by the major states that are active in the cyber norms debate are unanimous that cybercrime poses a threat to international peace and security.[5] Cybercrime is, therefore, a global challenge that can best be tackled by a concerted effort at the international law level.[6] This is because, as far as cybercrimes are concerned, the issue is no longer that of "a country protecting its own security, it is a question of the global community protecting itself".[7]

It is now fairly settled that international law applies to cyberspace and that existing international legal provisions can provide sufficient guidance and guarantees for states' relations in cyberspace.[8] According to the United Nations Governmental Group of Experts

[1] D.G. Post, "Against 'Against Cyberanarchy" (2002) 17 *Berkeley Tech Law Journal,* 1365 - 1387.
[2] 'Cyber-attack: US and UK blame North Korea for WannaCry' *BBC* 19 December 2017.
[3] A. Peters, A. Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime" (2020) *Journal of National Security and Law and Policy*, Vol. 10:487, pp. 490-492.
[4] United Nations, *Comprehensive Study on Cybercrime* (UNODOC; New York, 2013) p.117.
[5] Global Commission on the Stability of Cyberspace *ISSUE BRIEF. No.1 GCSC* (New Delhi, 2017) p. 30.
[6] J. Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization" (2016) 40 (3) *Monash University Law Review* 698-736, p. 699.
[7] S. Schjolberg, "Crossing jurisdictional boundaries" (2014) Europol-INTERPOL Cybercrime Conference. The Hague, p. 3.
[8] E.T. Jensen, S. Watts, (2021) "Cyber Due Diligence" (2021) 73 *Oklahoma Law Review*, 645, p. 691. Available at https://digitalcommons.law.ou.edu/olr/vol73/iss4/3 (accessed 4 August 2023).

(UNGGE), [9] "International law, in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment."[10] The Tallinn Manuals[11] even outlined how existing international law applies to cyberspace, and proposed specific rules that states "should follow to remain compliant with international law". [12] Further, the United States International Strategy for Cyberspace recognizes that "the development of norms for state conduct in cyberspace does not require a reinvention of customary international law**,** nor does it render existing international norms obsolete", and that long-standing international norms guiding state behaviour also apply in cyberspace.[13]

## 1.2 Nation-States as the Medium of International Law Application

The principles of international law are ultimately applicable through national-law-based state action.

> The traditional international law approach is to operate on the state level through international treaties and customs, entailing state duties that are to be later implemented against private actors through national laws and regulations.[14]

Against this background, it has been proposed that with the United Nations at the centre, cyberspace governance should be by both sovereign states and the international community. For one, the orderly functioning of cyberspace concerns the interests of all states as each "state is entitled to the exercise of sovereignty over cyber infrastructure, online data, cyber activities, and cyber governance

[9] UNGGE 2012/2013 Consensus Report, Adopted via UN General Assembly Resolution A/RES/68/243.
[10] *Supra* note 8 at p. 685.
[11] M.N. Schmitt, (ed) *Tallinn Manual on The International Law Applicable to Cyber Warfare 1.0* (Cambridge University Press; Cambridge, 2013); M.N. Schmitt, (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, (Cambridge University Press; Cambridge, 2017); see also E.T. Jensen, "The Tallinn Manual 2.0: Highlights and Insights", (2017) 28 *Georgetown J of Int'l Law* pp. 735-778.
[12] *Supra* note 5 at p. 28.
[13] G. Brown, K. Poellet, "The Customary International Law of Cyberspace", (2012) 6 *Strategic Studies Quarterly* No. 3:126-145, p. 140.
[14] *Supra* note 5 at p. 89-90.

within its own territory".[15] This state of affairs should naturally endow states with the power to exercise extra-territorial jurisdiction over cyber activities pursuant to international law.

According to the Tallinn Manual, a state enjoys:

> sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.[16]

Two international law consequences follow from this. First, the cyber infrastructure in a state and the activities it enables are subject to domestic legal and regulatory control by the state. Pursuant to this principle,

> States have the right to disconnect from the Internet, in whole or in part, any cyber infrastructure located on their territory. Second, the state thereby has the right under international law to protect cyber infrastructure and safeguard cyber activity that is located in or takes place on, its territory.

There is, therefore, some tenable ground for asserting as a matter of international norm that states "can establish an international control over the internet, and restrict internet access within their own borders.[17] Also, the development of customary international law is largely along the lines of state action (or inaction) in published government materials, domestic laws, and court decisions that detail actual practice. Over time, specific instances of state practice may develop into a general custom.[18] In fact, the current trend is that "in the absence of formal globally binding international agreements, cyber custom is beginning to develop through the practice of states".[19]

---

[15] M. Xinmimm, "Key Issues and Future Development of International Cyberspace Law" (2016) 2 *China Quarterly of International Strategic Studies*, No. 1:119–133 DOI: 10.1142/S2377740016500068.

[16] Rule 2, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Supra* note 11 at p. 3.

[17] *Supra* note 7.

[18] *Supra* note 13 at p. 127.

[19] *Supra* note 13 at p. 141.

It can be seen against this backdrop that the legal framework put in place by Nigeria to address cybercrimes is significant for international law purposes. On the one hand, the framework will help the country secure its domain from the vulnerabilities to which countries are exposed in cyberspace, to maximise its exploration of the benefits afforded by the digital space and, consequently, achieve growth effects on the overall economy. On the other hand, how the country fared in dealing with domestic cybercrime has important international implications. The most important of these is the country's *state responsibility* under international law[20] to ensure that cyber activity originating from its territory does not cause transboundary harm affecting other territories. As an index of the country's performance in dealing with cybercrime, it has been reported that about 25 percent of its cybercrime cases are unresolved, that 7.5 percent of the world's hackers are Nigerians, and that the country is the 3rd in the world after the US and UK in global internet crime.[21] This bleak picture negatively affects the country's standing in the comity of nations as well as its voice as a regional power on the African continent. The Cybercrime (Prohibition, Prevention, etc.) Act 2015 holds great promise in turning things around for the country.

The Act has the primary objective of providing an effective, unified, and comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. It also aims to ensure the protection of critical national information infrastructure (CNII), promotion of cybersecurity, protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights.[22]

---

[20] See generally J. Kulesza, *Due Diligence in International Law* (BRILL, 2016). pp. 221-258.

[21] A. Adepetun, '25% of cybercrime cases unresolved' *The Guardian* (Lagos, September 1 2015). www.guardian.ng/technology/25-of-cybercrime-cases-unresolved/ (accessed August 8 2023).

[22] *Cybercrime (Prohibition, Prevention, etc.) Act, 2015,* s.1.

Although there is an appreciable mass of literature on the celebrated Nigerian Cybercrime legislation**,** almost all the works do not look at the Act in the light of international law. The literature overwhelmingly focuses on analyses of individual cybercrime provisions, the accompanying enforcement framework, and the overall within-border impact of the law.[23] The modestly novel objective of this paper is to look at the above aspects of the Act but through the lens of the emerging international cyberspace law. Part I kickstarts the paper by highlighting the transnational nature of cybercrime as well as identifying the important place of national legislation in the global framework for the fight against the crime. Part II looks at the issue of criminalization, first, at the national level so as to capture the whole range of harmful cyber activities, and, second, the harmonisation of such legislation at the international level so as to reduce divergences among them. Part III considers the provisions of the Act with respect to the protection of critical information infrastructure (CII) as a means to discharge the country's state responsibility under international law to guard against cyber activity that may negatively affect other countries. Part IV discusses the subject of international cooperation in dealing with cybercrimes and the relevant provisions made by the Act for that purpose. Part V identifies the provisions of the Act to enable Nigeria assert its jurisdiction on cybercrimes, while Part VI wraps up the discussion.

## 2.0 INTERNATIONAL CYBERSPACE LEGISLATION

The cybercrime challenge has elicited an impactful response from the United Nations, the Organisation for Economic Cooperation and Development (OECD), the Commonwealth, the Council of Europe, the European Union,[24] the African Union, the Economic Community of West Africa (ECOWAS), and many other international and

[23] See for example A. Adekunle, (ed) *Combating Cybercrimes in Nigeria: Trends and Issues*. (NIALS; Lagos, 2017); N. A. Duson, S.D. James, "Cyberterrorism and the Protection of Critical Information Infrastructure in Nigeria: A Legal Assessment" (2020) 8(3) *Int'l Journal of Innovative Legal and Political Studies*, 25-36, 33.

[24] F. Calderoni, "The European legal framework on cybercrime: striving for an effective implementation" (2016) *Crime, Law and Social Change*, 54(5) 339-357, p. 1.

regional institutions. With respect to legislation, the Council of Europe made the first input in its *Convention on Cybercrime*[25] which proposed a standard of offences according to which states may model their cybercrime laws.[26] The *Convention* sets out the core of internet crimes generally described as crimes against the confidentiality, integrity, and availability (CIA) of computer data and systems. [27] More comprehensively, the *Convention* requires the criminalization of conduct that falls into one of four categories: offences against the confidentiality, integrity, and availability of computer systems; computer-related offences (e.g. forgery, fraud); content-related offences (e.g., child pornography); and offences related to the infringement of copyright and related rights.

Along the same lines, the Economic Community of West Africa (ECOWAS) *Directive on Fighting Cybercrime* called on African states to criminalise wrongful cyber conduct in their respective domains.[28] Also, the yet-to-be-enforced African Union *Convention on Cyber Security and Personal Data Protection* requires every African state to, inter alia, consider as substantive criminal offences acts which affect the

> confidentiality, integrity, availability and survival of computer systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders.[29]

## 2.1 The Need for Harmonization

As countries began to pass cybercrime laws, differences in their legislations began to emerge, leading to complications in interstate

[25] Nigeria acceded to the Convention on 6, July 2022. See Z.Z. Usman "Monguno Announces Nigeria's Accession to the Budapest Convention on Cybercrime" available at https://prnigeria.com/2022/08/22/monguno accessed August 22 2022.
[26] A. Adekunle, "A Review of the Cybercrime Act 2015" In A. Adekunle, (ed) *Combating Cybercrimes in Nigeria: Trends and Issues* (NIALS; Lagos, 2017) p. 13.
[27] *Supra* note 24 at p. 4.
[28] Economic Community of West Africa *Directive on Fighting Cyber Crime within Economic Community of West African States 2011* (ECOWAS Directive). Article 2.
[29] African Union, African *Union Convention on Cyber Security and Personal Data Protection, 2014* EX. CL/846(XXV). Article 25(1).

investigation, prosecution, and punishment of offenders. These differences in "legal systems and attendant substantive and procedural laws of various jurisdictions have hindered the effective enforcement of cybercrime laws at the international level,"[30] most notably by creating safe havens where cybercriminals can freely engage in their acts without fear of being caught up by the law, and by giving rise to intricate conflict of law issues. There was a clear need to harmonise those legislations. Based on the understanding that "one of the aims of international law is to achieve harmonisation of national laws," the trend, therefore, changes to that of removing such differences in national legislations.[31]

It became necessary "to harmonise penal codes through guidelines or recommendations to assure proper prosecution, which otherwise could be prevented by international jurisdictional problems."[32] The UN *Convention Against Transnational Organised Crimes* (UNCTOC) had earlier identified the need with respect to crimes generally, enjoining states to harmonise their criminal laws on the various organised criminal activities.[33] The African Union brought this proposal home through its *Convention on Cybersecurity and Personal Data Protection,* which called on African states to harmonise their cybercrime legislation[34] to, among other things, "respect the principle of double criminal liability."[35]

The principle of *dual criminality* lies at the centre of international cooperation in the fight against cybercrime and raises the question of whether conduct amounting to cybercrime in one country is also criminalised in other countries affected by the conduct.[36] Without this duality or equivalence between cybercrime laws in two or more

[30] P.T. Akper, A.O. Aderiran "Cybercrimes and the International Legal Order" In *Supra* note 23 at p. 23.
[31] *Supra* note 4 at p. 8.
[32] *Supra* note 7 at p. 3.
[33] I.O. Ifeakandu "Challenges in the Detection and Prosecution of Cybercrimes" In *Supra* note 23 at p. 179.
[34] See Article 28.
[35] *Supra* note 30 at p. 37.
[36] *Ibid.*

states, international cooperation, mutual legal assistance, extradition, etc., will not succeed.[37] Failure to ensure equivalence amongst national cybercrime laws is utilised by cybercriminals to their advantage. The case of *United States* v *Gary McKinnon*[38] illustrates the sort of problems occasioned by such divergences. McKinnon, a systems administrator in the UK, unlawfully gained access to 97 US military and National Aeronautics and Space Administration (NASA) computers from his home computer. Charges were filed in the US states of Virginia and New Jersey, resulting in the issuance of an arrest warrant against him. In order to escape the 70-year term of imprisonment under US law, as against the only five years under the UK *Computer Misuse Act*, McKinnon fought and successfully avoided extradition to the US with his lawyers rightfully arguing that the location of the criminal act, the facilities and the computers used were all located in the UK.[39]

## 2.2 Nigeria's Cybercrime Offences

The Nigerian Cybercrime Act's criminalization of cyber activities identified as the most injurious at the international level will go a long way in ensuring that the investigative, prosecutorial, and enforcement challenges outlined above are not encountered in the event of a cybercrime incident involving the country. The catalogue of offences it contains follows, generally, the recommendations of the ECOWAS *Directive* and, more closely, the Council of Europe Convention's model. But it goes beyond the latter by featuring cyber terrorism as a cybercrime, which does not appear even in the Convention's *Additional Protocol*.[40] In this, the Act follows the ECOWAS *Directive,* which obliges state parties to criminalise the use of ICT to commit terrorism and to treat it as "a higher degree of offence than the common law offences."[41]

[37] *Supra* note 24 at p. 14.
[38] [2007] EWHC 762 (Admin) - Casemine.
[39] *Supra* note 39 at p. 28.
[40] *Supra* note 23 (a) at p. 11.
[41] *ECOWAS Directive*. Article 25.

Adewopo[42] has distilled a total of 26 offences in the Act (each of which is capable of subsuming a number of other offences) categorizable into the two generally agreed classification of cybercrimes: those that *target* computer systems and data, and those involving the *use* of the said systems and data as tools to commit conventional crimes.[43] Cybercrimes of the first category include unlawful interference with critical national infrastructure,[44] unlawful access to a computer,[45] unlawful interception of computer communications,[46] unlawful alteration or destruction of computer data; interference with a system or network of computers, and misuse of devices.[47] Those of the second category include computer-related crimes such as fraud,[48] forgery,[49] impersonation,[50] pornography,[51] terrorism,[52] and the dissemination of racist or offensive material.[53]

The overall effect of criminalising wrongful cyber activities at the national level and harmonising them at the international level is that cybercrime anywhere in the world will be effectively captured, with the ground cleared for international cooperation and mutual legal assistance toward bringing perpetrators to justice. The Nigerian *Cybercrime Act* is therefore very significant in this respect by enabling the country to pose in concert with other global players toward facing down the international menace.

[42] A. Adewopo "Critical Analysis of Intellectual Property Rights under the Cybercrime Act 2015" In *Supra* note 23 at p.74.
[43] *Supra* note 24 at p. 4.
[44] *Cybercrime Act* ss. 3 and 5.
[45] Cybercrimes (Prevention, Prohibition, etc) Act, 2015, s. 6.
[46] Cybercrimes Act 2015, ss. 9 and 12.
[47] Cybercrimes Act 2015, s. 28.
[48] Cybercrimes Act 2015, s. 14.
[49] Cybercrimes Act 2015, s. 13.
[50] Cybercrimes Act, 2015, s. 22.
[51] Cybercrimes Act, 2015, s. 23.
[52] Cybercrimes Act, 2015, s. 18.
[53] Cybercrimes Act, 2015, s. 26.

## 3.0 CRITICAL INFRASTRUCTURE PROTECTION AND GLOBAL CYBERSECURITY

The Global Commission on the Stability of Cyberspace (GCSC), in its 2017 briefing, listed Nigeria as one of the four African countries and one of 38 countries globally with a legal definition of *Critical Information Infrastructure.*[54] This is based on the description, given under Section 58 of the Cybercrime Act, of critical information infrastructure as:

> certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

In capturing offences against critical national information infrastructure (CNII), Section 5 of the Act provides that:

> Any person who, with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to section 3 of this Act, shall be liable on conviction to imprisonment for a term of not more than 10 years without option of fine.

### 3.1 Critical Information Infrastructure Dependencies

Critical information infrastructure broadly means "ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures." [55] Critical information infrastructure also includes "systems of electronic devices, computers and communication networks, essentially integrated to improve the synergy, productivity, efficiency, and performance of critical infrastructure or critical national infrastructure."[56] Because of the interconnectedness of the internet, dependencies amongst these

[54] *Supra* note 5.
[55] D. Clemente *Cyber Security and Global Interdependence: What is Critical ?* (Chatham House; London, 2013) p.16.
[56] U.M. Mbanaso, V.E. Kulugh, J.A. Makinde "A Framework for the Determination of Critical National Information Infrastructure in Nigeria" (2020) 4 *Journal of Information Science, Systems and Technology* p. 2.

infrastructures are bound to occur. Infrastructure dependency is a situation of "one-directional reliance of an asset, system, network, or collection thereof — within or across sectors — on an input, interaction, or other requirement from other sources in order to function properly."[57] It describes a situation of infrastructures and systems having "to interconnect, integrate, and drive the other critical traditional infrastructure." [58] In this complex mix of interconnectedness, a disruption in one infrastructure component may affect all other components simultaneously.

More pertinent to the theme of this paper is cross-border dependency, critical infrastructure dependencies among information infrastructures beyond the national territory. At the lowest level, internet and communication service providers, who are characteristically transnational, "spatially define the external limits of a country's national security." [59] This means that there is a relationship of critical dependency between Nigeria's critical information infrastructure and that of a transnational service provider, say MTN, located outside the border in South Africa. The critical infrastructures of other countries in Africa that are dependent on the parent infrastructure in South Africa are all open to the vulnerabilities it carries, just as a vulnerability in any state link along the chain of dependency is a vulnerability of the entire dependency chain. It can be seen here that the "resilience of interconnected critical infrastructure nationally also depends critically on the security and reliability of global cyber networks, which themselves are vulnerable as prey targets of cyber-attacks."[60] This picture has prompted the conclusion that "participation in the global infrastructure ecosystem is inherently predicated on acceptance of a measure of unknowable risk."[61]

[57] K. Kaska, L. Reinberg *Regulating Cross-Border Dependencies of Critical Information Infrastructure* (CCDCOE; Tallinn, 2015) p. 15.
[58] *Supra* note 56 at p. 4.
[59] *Supra* note 55 at p.14.
[60] *Supra* note 56 at p. 2.
[61] *Supra* note 55 at p. 9.

### 3.2 Critical Information Infrastructure Vulnerabilities and State Responsibility

Risks and vulnerabilities inherent in critical information infrastructures could take the form of disruptions which may "be caused by any number of factors e.g. poor design, operator error, physical destruction due to natural occurrences (flood, earthquake, etc.), or physical destruction due to intentional human actions (terrorist attacks, theft, vandalism, untoward interventions, etc)."[62] Alongside the apparent domestic necessity, putting in place legal and institutional frameworks to guard against these disruptions is significant in terms of the country's *state responsibility* under international law. This is because a disruption originating from Nigeria's infrastructure (as a result of it being attacked or vulnerabilities in it being exploited to attack other infrastructure) may affect interconnected infrastructures in other countries, which may result in harm to those countries that may qualify as transboundary harm under international law.

The obligation under customary international law for states to prevent transboundary harm has been held to be applicable to cyberspace.[63] There is, therefore, an international responsibility on states to protect cyber infrastructure located in their territory from being used in a manner that is injurious to the rights of other states. According to the Tallinn Manual, a state "shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States".[64] States must accordingly take the necessary steps to prevent harm that may result from misuse or damage to infrastructure located within their borders and over

[62] Industry Working Group on Multiple Taxation. "Brief on the Designation of Telecommunications Infrastructure as Critical National Infrastructure," p. 2. available at http://www.ncc.gov.ng/documents/248-brief-on-the-designation-telecommunications-infrastructure-as-critical-national-infrastructure/file (accessed April 4 2022).

[63] See generally R.J. Buchan "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm" (2015) *Journal of Conflict & Security Law,* 21 (3), 429-453, available at https://doi.org/10.1093/jcsl/krw011 (accessed August 4 2023.)

[64] Rule 5. *Supra* note 11a at p. 33.

which they exercise territorial sovereignty. This is achieved by discharging two obligations: an *obligation of result* by which they implement laws and institutions that are capable of preventing their territory from being used in such a way as to violate the legal rights of other states and, an *obligation of conduct* in the sense that where a threat emerges, and they have (actual or constructive) knowledge of that threat, they must act reasonably in utilising their capacity and resources to suppress it. Both obligations include states engaging in capacity building by equipping themselves with the means to detect, prevent, mitigate, and punish conduct by non-state actors within their territory that is contrary to the international law rights of other states. This boils down to "the enacting of legislation and regulations and the establishment of an effective administrative and judicial apparatus."[65]

Imposing such special obligations under international law is usually done through the means of treaties. In the context of malicious cyber activity by non-state actors, the Council of Europe *Convention* requires states parties to adopt "legislative and other measures" to ensure that the offences listed therein are "punishable by effective, proportionate and dissuasive sanctions." This is very significant as the borderless character of cyberspace, its inherent interconnectedness, and the anonymity it affords, has provided a thriving environment for non-state actors to act ever more independently from states in the international arena. It is even feared that harmful transboundary cyber conduct on the part of non-state actors may exceed that on the part of states.[66]

### 3.3 Nigeria's Input Towards Global Cybersecurity

In this context, the Nigerian Act and its institutional framework will help enhance the country's cyber resilience by reducing risks and vulnerabilities in its critical information infrastructures. It will also go a long way in reducing the risk of cyber criminals and other non-state actors exploiting vulnerabilities in the country's critical infrastructures to cause transboundary harm. This is in line with

[65] *Supra* note 63 at p. 11.
[66] *ibid* at p. 3.

keeping with the customary international law obligations outlined above.

Harmful activities in cyberspace have been generally classified into those that unlawfully *target* computers, devices, and networks on the one hand and those that unlawfully *use or misuse* computers, devices, and networks on the other.[67] Activities in the first category are more likely to constitute problems as far as the security of critical information infrastructure is concerned, and the Nigerian Act can be said to have fairly addressed this challenge by looking at the list of cyber activities it criminalises. Most notable is the constellation of offences in Sections 3-10, including unlawful interference with critical information infrastructure, unlawfully accessing computer devices, unlawful alteration or destruction of computer data, interference with a system or network of computers, unlawful interception of computer communications, etc.

Part of the international best practice in cybersecurity is the carrying along of operators and owners of information infrastructure who have to plan and apply security measures, manage risks in the infrastructure in their operation, and ensure the functioning of installations, networks, systems, and physical or ICT assets. They also have the obligation to keep proper documentation, report attacks, and submit to government guidelines in the case of incidents. [68] Accordingly, the Nigerian Act provides that these operators shall immediately inform the National Computer Emergency Response Team (CERT) Coordination Centre of any attacks, intrusions, and other disruptions liable to hinder the functioning of another computer system or network.[69] Operators of cybercafés, which in most cases constitute vulnerability nodes[70] as well as points for carrying out unlawful activities on the internet, are required to register as businesses with the Computer Professionals'

[67] *Supra* note 23 at p. 3.
[68] *Supra* note 55 p. 13.
[69] Cybercrimes Act, 2015, s. 21(1).
[70] These are "points in a system where failure would significantly degrade the network" *Supra* note 55 at p. 17.

Registration Council (CPRC) in addition to business name registration with the Corporate Affairs Commission (CAC). They are also mandated to maintain a users' sign-in register, which shall be available to law enforcement personnel whenever needed.

According to Section 10 of the Act, any person who, in the course of his employment with respect to working with any critical infrastructure, commits any act which he is not authorised to do by virtue of his contract of service, or intentionally permits tampering with any computer, is guilty of an offence. And to ensure overall compliance with the Act, Section 4 provides for audits and inspection of critical national information infrastructures by the Office of the National Security Adviser (ONSA) by a presidential order to that effect.

Strengthening the provisions of the Act, the Nigerian Cybersecurity Policy and Strategy [71] articulates the various activities to be undertaken towards the protection of critical national information infrastructure. At the core of the strategy is the Critical Information Infrastructure Protection and Resilience (CIIPR) framework, which is based on the collective participation of stakeholders in the public and private sectors. Risks to critical information infrastructures will be proactively assessed through an intelligent and information-led risk management approach, which will lead to their being secured against physical, human, and cyber threats through collective and sustainable efforts.[72]

A preliminary requirement identified by the strategy for the CIIPR is the identification of critical infrastructure *sectors* and appropriately categorising them in accordance with their priority for protection based on their vulnerability and impact assessment. The strategy provides that the appropriate authorities shall keep and continually update a comprehensive list of critical infrastructures that require protection priorities. [73] Accordingly, the strategy identifies the

[71] Federal Republic of Nigeria *National Cybersecurity Policy and Strategy 2021*.
[72] *Ibid* at p. 20.
[73] *Ibid*.

following 13 critical infrastructure sectors: Power and Energy; Water; Information, Communications, Science and Technology; Banking/Finance and Insurance; Health; Public Administration; Education; Defence and Security; Transport; Food and Agriculture; Safety and Emergency Services; Mines and Steel; Industrial and Manufacturing.[74] And pursuant to powers to designate certain assets, services, facilities, or systems as critical national information infrastructure, and accord them adequate national protection, the President has accordingly designated some communications infrastructures as such.[75] This is a commendable first move because communications infrastructures are critical national assets that warrant the highest level of protection, given their significance to the efficient functioning of the society.[76]

## 4.0 INTERNATIONAL LEGAL COOPERATION ON CYBERCRIME

Bringing to justice the perpetrators of cybercrimes is a transnational process involving the cooperation of numerous law enforcement bodies. Cooperation among states is, therefore, necessary if the states are to succeed in this endeavour.[77] In so far as investigations may involve other states, processes of consent and mutual cooperation are necessary. Many of these processes are provided for in bilateral or multilateral treaties, although national laws can specify procedures to be applied or even create bases for cooperation in their own right.

The prosecution of transnational acts requires states to assert two types of jurisdictions: the substantive and the investigative. Substantively, states "must be able to assert that their national criminal law applies to an act that takes place only partly, or even not at all, within its national territory." By the investigative jurisdiction, they must "be able to carry out investigative actions that concern the

[74] *Ibid* at p. 21.
[75] *Supra* note 56 at p. 2.
[76] *Supra* note 62 at p. 2.
[77] *Supra* note 3 at p. 488.

territory of other states."[78] With respect to the former, states can make criminal law provisions that govern their citizens even when the citizens are abroad. This means that a Nigerian citizen, for example, can be prosecuted for cybercrime committed in another country even if the conduct did not have any harmful effect in Nigeria as the prosecuting country.[79] But typical of challenges posed by jurisdictional issues, usually, even where cybercriminals are detected, arresting and taking them into custody and prosecuting them could be difficult in the absence of some form of cooperation framework between the arresting authority and the country where the criminal is found.

### 4.1 The Enabling Provision for International Cooperation

Laying the ground for Nigeria's participation in international legal cooperation on cybercrimes, Section 52(1) of the Act provides that:

> The Attorney General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence.

Making things simpler and easier, the joint investigation or cooperation envisaged above may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country.[80] In terms of the request for mutual assistance, the Attorney General may, without prior request, forward to a competent foreign authority information obtained in the course of investigation if such information will assist in the investigation of an offence or in the apprehension of an offender.[81]

In order to coordinate outgoing and incoming requests for extradition and mutual legal assistance, the international practice involves states designating "a 'central authority' with the power to

[78] *Supra* note 4 at p. 55.
[79] *Supra* note 33 at p. 178.
[80] s. 52(2).
[81] s. 52(3).

receive requests and either to execute them or to transmit them to the competent authorities".[82] Besides the Attorney General of the Federation of Nigeria who constitute such central authority, the Act provides that in "order to provide immediate assistance for the purpose of international cooperation, the Office of the National Security Adviser shall designate and maintain a contact point that shall be available" seven days a week, and that this "contact point can be reached by other contact points in accordance with agreements, treaties or conventions by which Nigeria is bound, or in pursuance of protocols of cooperation with international judicial or law enforcement agencies."[83]

### 4.2 Preservation of Data for Investigative Purposes

On the dogged question of preservation of data stored in a computer system referring to an alleged cybercrime, the Act provides that law enforcement agencies in Nigeria "may be requested to expedite the preservation of electronic devices or assistance for search, seizure, and disclosure of those data."[84] In "executing the demand of a foreign authority, the Attorney General of the Federation may order any person who has the control or availability of such data, including a service provider, to preserve them or turn them in for proper preservation by an appropriate authority or person.[85]

The Act also made further general provisions to enable Nigeria to adequately fit into the global cybercrime control network. The Attorney General of the Federation is mandated to "strengthen and enhance the existing legal framework to ensure conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards." The Attorney General is also obligated to ensure the "maintenance of international cooperation required for preventing and combating cybercrimes and promoting

[82] *Supra* note 4 at p. 186.
[83] s. 56(1).
[84] s. 55(1).
[85] s. 55(3).

cyber security; and effective prosecution of cybercrimes and cyber security matters."[86]

### 4.3 Extradition of Cybercrime Suspects to and from Nigeria

Extradition "involves the formal surrender of a person by one state for the purposes of prosecution or for the imposition or enforcement of a sentence in another" state.[87] Normally, states are not under obligation to hand over a suspect to a requesting state or entity except where a specific extradition treaty has been agreed upon. Where a country "is party to such agreements, the procedure to be followed in processing both incoming and outgoing requests is often set out in national law. In addition, in some countries, domestic law may itself provide the basis for international cooperation in place of reliance upon a treaty."[88] Although the Nigerian *Cybercrime Act* does not constitute such domestic law, it covers the field by incorporating into its framework the existing extradition procedure under the *Extradition Act*. Section 51 of the Act provides that "Offences under this Act [the *Cybercrime Act*] shall be extraditable under the Extradition Act."[89] The country is thereby endowed with the necessary legal ground to request from another country the enforced return of a cybercrime suspect, as well as receive similar requests from other countries**.**

## 5.0 THE QUESTION OF JURISDICTION IN CYBERSPACE

A state's exercise of jurisdiction is conceived of as taking one of three forms: exercise of jurisdiction in prescribing or enacting law; exercise of jurisdiction in adjudicating or subjecting persons or entities to its law and; exercise of jurisdiction in enforcing compliance with its law.[90] The two bases upon which this exercise of

[86] s. 41(2).
[87] *Supra* note 6 at p. 707.
[88] *Supra* note 4 at p.186.
[89] CAP E25, Laws of the Federation of Nigeria, 2004.
[90] D.E. Stigall "International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law" (2012) 35 *Hastings International & Comparative Law Review* p. 328.

jurisdiction are founded under international law are *territoriality* and *nationality*. The former confers jurisdiction on the state in which the person or the subject matter in question is situated or in which the event in question took place. The latter confers jurisdiction over nationals of the state concerned.[91]

## 5.1 The Nature of Jurisdiction in Cyberspace

The virtual nature of cybercrime requires the establishment of clear rules on the exercise of jurisdiction in appropriate cases. Further, because cybercrimes typically have effects in different places under the jurisdiction of different countries, there is a strong need for clear norms setting the priorities and competencies of each country involved.[92] Under the emerging international cyberspace law, the right of states to exercise jurisdiction over cyber infrastructure and over related cyber activities is pursuant to the principle of *territorial sovereignty*. Territorial sovereignty confers on a state territorial jurisdiction, enabling it to regulate, restrict, or prohibit access to its cyber infrastructure, whether access is gained from within or without its territory.[93] In other words, cyber infrastructure located within the territory of a state, and cyber activities occurring therein are subject to the prescriptive, adjudicative, and enforcement jurisdictions of the state concerned.

However, the exercise of jurisdiction is not limited to a state's territory. For instance, a state exercises exclusive jurisdiction on board a vessel flying its flag and on board an aircraft registered in that state. Moreover, according to the *nationality* principle, a state is entitled to exercise jurisdiction over conduct that occurred outside its territory (based on the effects doctrine) on the basis of the fact that either the perpetrator or the victim is its citizen. And under the *universality* and *protective* principles, a state can exercise jurisdiction even if neither the perpetrator nor the victim is its citizen.[94] The

[91] W. Von Heinegg "Territorial Sovereignty and Neutrality in Cyberspace" (2013) *89 Int. Law Studies* 123, pp. 132-134.
[92] *Supra* note 24 at p. 3.
[93] *Supra* note 91 at p. 133.
[94] *ibid* at 132.

Council of Europe Convention's *Explanatory Report* clarifies that under the principle of *territoriality*, a state would assert territorial jurisdiction if both the attacker and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not.[95]

As the main model of international cybercrime law, the Council of Europe *Convention on Cybercrime* provides that in terms of substantive jurisdiction, states must enact legislation to enable them to actively assert jurisdiction over criminal offences. Within its particular limits, the Convention requires state parties to establish jurisdiction over the offences it sets out under Articles 2–11 when the offences are committed a) within their territories, on board a ship or aircraft flagged or registered under their laws, or b) by one of their nationals if the offence is punishable under the criminal law where it was committed, or c) if the offence is committed outside the territorial jurisdiction of any state.[96]

The above provision of the *Convention* applies the principles of jurisdiction outlined above, i.e., the principles of territoriality, nationality, protective, and universal principles. It is also along the same line that the Nigerian *Cybercrime Act* makes the provision to enable the country to effectively assume jurisdiction over cybercrimes affecting either its territory or involving its citizenry. Section 50 of the Act provides as follows:

> The Federal High Court of Nigeria shall have jurisdiction to try offences committed
> (a) in Nigeria; or
> (b) in a ship or aircraft registered in Nigeria; or
> (c) 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; or
> (d) outside Nigeria, where -
> (i) the victim of the offence is a citizen or resident of Nigeria; or

[95] *Supra* note 4 at p. 191.
[96] *Supra* note 6 at p. 706.

(ii) the alleged offender is in Nigeria and not extradited to any other country for prosecution.

With this provision, Nigeria, in the event of a call to that effect, can effectively assert jurisdiction on any cybercrime on all the outlined bases of jurisdiction namely: territorially, extraterritorially, as well as under the protective and universal principles, barring only its capacity to effectively investigate and prosecute.

## 6.0 CONCLUSION

This article has pinpointed some of the main provisions of the Nigerian *Cybercrime Act,* 2015 that are very relevant in the emerging scheme of international cyberspace law. Like similar legislations enacted in other internationally active countries, the Act sufficiently puts Nigeria in the position to assume jurisdiction over cybercrime incidents involving it regardless of the physical location of the actors and the subject matter(s) concerned. Thanks to the Cybercrime Act, the country can also properly engage in international legal cooperation and mutual legal assistance processes with other countries toward the investigation, arrest, extradition, prosecution, punishment, etc., of suspected cyber criminals. On the whole, the Act makes it possible for the country to stand up to its state responsibility under international law to secure its cyber infrastructure and to deal with harmful cyber incidents relating thereto. This, ultimately, is an important contribution to global cybersecurity. It should be noted, however, that the provisions of the Act having some relevance to international law are, to a large extent, foundational. There is a big room for enhancement in terms of the individual substantive provisions, the institutional structures needed to effectively enforce them, and the manpower expertise needed to carry out the enforcement.

It is also noteworthy that the significance of the present paper lies only in the fact that it breaks the ground by looking at the *Cybercrime Act* exclusively from the angle of international law. This is extremely important because of the inherently transnational nature of cybercrime, a feature that seriously reduces the significance of any

discussion of the cybercrime problem in strictly nationalised terms. Intensive further research from this angle is therefore needed to more deeply evaluate the provisions of the Act toward better understanding, enforcement and possible future amendments.