ACCEDING TO INTERNATIONAL CYBERSECURITY CONVENTIONS

O. M. Atoyebi, S.A.N
Managing Partner, Omaplex Law Firm
atoyebi@omaplex.com.ng

In today's world, both states and non-state actors have become increasingly dependent on computers and the networks that connect them for the performance of many of their functions. As the reliance on digital technology grows, the impact of failure in networks and information systems and the opportunities for those who seek to compromise those systems increase. The global community continues to experience an increase in the scale, sophistication, and successful perpetration of cyber-attacks. As the quantity and value of electronic information have increased, so too has the effort of criminals and other malicious actors who have embraced the internet as a more anonymous, convenient, and profitable way of carrying out their dubious activities. According to Nexusguard- a cybersecurity company, in the first half of 2021, a distributed denial-of-service attack (DDoS)—being a malicious and targeted attempt to disrupt traffic to a particular server, service, or network—increased by 233%.[1]

Threats in cyberspace are difficult to define, as it is hard to identify the source of attacks and the motives that drive them, or even foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty of defining the boundaries between national, international,

[1] (Natalie Bannerman, DDoS attacks increase by 233% in 2021, finds Nexusguard, 2021 https://www.capacitymedia.com/articles/3829813/ddos-attacks-increase-by-233-in-2021-finds-nexusguard, accessed 29th November 2021)

public, and private interests. Because threats in cyberspace are global and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated. Threats to society's vital functions may directly or indirectly target national systems and/or citizens, from within or outside the national borders.

In 2018 alone, commercial banks in the country lost about N15 billion to electronic fraud and cybercrime, while over 17,600 bank customers lost N1.9 billion to cyber fraud in the same year. This is partly why, according to an African security study by De Madiur Systems Limited, a whopping sum of N270.22 million was spent by banks, insurance companies, and government institutions to prevent cyberattacks in the year 2018. These funds went to purchases of hardware and software like antivirus, load balancers, and network access controls, and even human investments like the hiring of cybersecurity experts. Also important to note is the report of the Nigeria Consumer and Financial Enlightenment Initiative, which projects that $6 trillion would be lost to cybercrime within and outside Nigeria by 2030. Cyber threats are not limited to banks and financial institutions but span across national and personal security, healthcare, retail, government agencies, and international relations, among others.[2]

The fight against cybercrime is borderless. States have rolled out frameworks that will help assuage the devastating effects of cybercrime. Likewise, the international community has developed frameworks, albeit not exhaustive, to help provide states with a blueprint to tackle the ever-growing menace of cybercrime. We, therefore look at these frameworks vis-à-vis Nigeria's cybercrime fight.

THE OBLIGATION OF STATES TO PREVENT INTERNATIONAL HARM TO CYBERSPACE

It used to be argued that cyberspace was a territorial and borderless environment separate from the physical and territorial demarcations that are subject to sovereign claims. Cyberspace was considered *sui generis,* without state authority or regulation. Practically, however, electronic information needs physical elements such as computers, routers, servers, and cables that are territorially based. Thus, states exercise sovereignty over those aspects of cyberspace that are supported by physical infrastructure based in their territory, encompassing their land area, their internal waters, their national

[2] (Babajide Komolafe, Over 17,600 bank customers lose N1.9bn to e-fraud in 2018, 2019 <https://www.vanguardngr.com/2019/05/over-17600-bank-customers-lose-n1-9bn-to-e-fraud-in-2018/)>

airspace, etc. The digital world does not constitute a new form of "outer space" where no state can exercise its jurisdiction but is subject to national and international laws. States have, in fact, regularly asserted their jurisdiction over cyber activities conducted in their territory.

It, therefore, follows that "international norms and principles that flow from sovereignty apply to state conduct of information and communication technology (ICT) related activities and their jurisdiction over ICT infrastructure within their territory" (UN Group of Governmental Experts (CGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, Report 2013 UN Doc. A/68/98, para. 20). In particular, the obligation upon states to prevent transboundary harm perpetrated within their territory or any other area under their exclusive control applies to harmful international conduct committed against the cyber-infrastructure located within their territory. Most states of the United Nations (UN) General Assembly called upon states to prevent their territory from being used as a haven from which to launch cyberattacks and to cooperate in the investigation and prosecution of such attacks (Resolution on Combating the Criminal Misuse of Information Technologies, 2001 UN Doc. A/RES/55/63, Art. 1).

The obligation to prevent harmful international operations also applies with regard to those operations launched from cyberinfrastructure that is outside a state's territory but is nevertheless under the exclusive control of the state, for instance in diplomatic premises or a state's airspace. According to **Rule 6 of the Tallinn Manual**[3]**,**

> **"[a] State must exercise due diligence in not allowing its territory, or territory or cyberinfrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other states."**

Furthermore, the obligation to prevent harmful international cyber activity does not only apply to the State from where the activity is launched but also to the State where the activity may transit.

[3] (The Tallinn Manual (originally entitled, Tallinn Manual on the International Law Applicable to Cyber Warfare) is an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare.)

GOVERNMENTAL EFFORTS IN DEALING WITH CYBERTHREATS

Cybercrime threats have received the attention of different organisations, from national and local governments to international organisations such as the Council of Europe and the United Nations, and non-governmental organisations (NGOs) dealing with issues such as privacy and human rights.

Several efforts have been made by various nations to create legislation concerning computer crime. The first was a federal bill introduced in 1977 in the U.S. Congress, although it was not adopted. The United States later passed the 1984 Computer Fraud and Abuse Law and the 1986 Computer Fraud and Abuse Act, which strengthened U.S. cyber-crime laws. Internationally, in 1983, the Organisation for Economic Co-operation and Development (OECD) made recommendations for its member countries to ensure that their penal legislation also applied to certain categories of computer crime.

The Thirteenth Congress of the International Academy of Comparative Law in Montreal, the U.N.'s Eighth Criminal Congress in Havana, and a conference in Wurzburg, Germany, all approached the subject in the early 1990s from an international perspective. The focus of these conferences included modernizing national criminal laws and procedures; improvement of computer security and prevention measures; public awareness; training of law enforcement and judiciary agencies; collaboration with interested organizations; and rules and ethics in the use of computers.[4]

In 1997, the High-Tech Subgroup of the G-8's Senior Experts on Transnational Organised Crime developed ten principles and a plan of action for combating computer crime. This was followed in 1999 by the adoption of principles of transborder access to stored computer data by the G-8 countries. The principles and action plans include:

- A review of legal systems to ensure that telecommunication and computer system abuses are criminalized;
- Consideration of issues created by high-tech crimes when negotiating mutual assistance agreements and arrangements;

[4] (Harold F. Tipton& Micki Krause, Information Security Management Handbook, Volume 4, Volume 4, Auerbach Publications) 830)

- Solutions for preserving evidence prior to investigative actions;
- Creation of procedures for obtaining traffic data from all communications carriers in the chain of communication and ways to expedite the passing of this data internationally;
- Coordination with industry to ensure that new technologies facilitate national efforts to combat high-tech crime by preserving and collecting critical evidence.

Around the globe, states are rapidly developing laws to combat cyber-crime, but the organization that has introduced the most far-reaching recommendations has been the Council of Europe (CoE). The **Convention on Cyber-Crime** was opened for signature on November 23, 2001. The impact of the treaty has the potential to be significant considering that CoE members and observing countries represent 80 percent of the world's internet traffic alone.

COUNCIL OF EUROPE CONVENTION

The objective of the Council of Europe's Convention on Cyber-Crime, also known as the ***Budapest Convention,*** is to create a treaty to harmonize laws against hacking, fraud, computer viruses, child pornography, and other internet crimes and ensure common methods of securing digital evidence to trace and prosecute criminals. It is the first international treaty to address criminal law and procedural aspects of various types of criminal behaviour directed against computer systems, networks, or data, and other types of similar misuse. Each member country is responsible for developing legislation and other measures to ensure that individuals can be held liable for criminal offences as outlined in the treaty. [5]

National Law:

At the national level, all signatory countries are expected to institute comprehensive laws concerning cyber-crime, including the following:

[5] European Treaty Series - No. 185 Convention on Cybercrime
Budapest, 23.XI.2001

- Criminalize "offenses against the confidentiality, integrity, and availability of computer data and systems," "computer-related offences," and "content-related offenses."

- Criminalize the "attempt and aiding or abetting" of computer-related offenses.

- Adopt laws to expedite the preservation of stored computer data and "preservation and partial disclosure of traffic data."

- Adopt laws that empower law enforcement to order the surrender of computer data, computer systems, and computer data storage mediums. This also includes subscriber information provided by an ISP.

- Adopt laws that provide law enforcement with surveillance powers over "content data" and require ISPs to cooperate and assist.

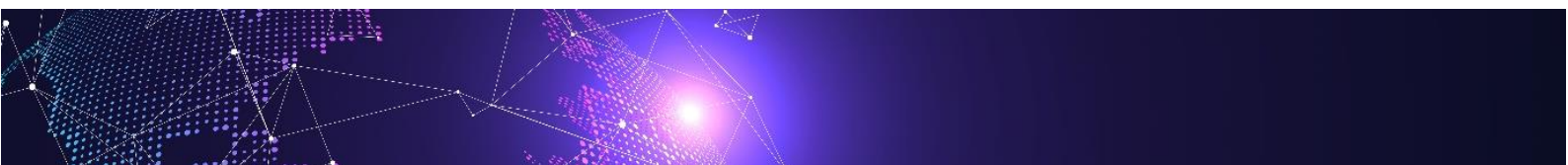
- Adopt legislation that establishes jurisdiction for computer-related offences.

International Cooperation:

The section of the convention dealing with “international cooperation” concerns the development and modification of arrangements for cooperation and reciprocal legislation. Some of the more instructive features include;

- Acceptance of criminal offences within the Convention as extraditable offenses, even in the absence of any formal extradition treaties. If the extradition is refused based on nationality or jurisdiction over the offense, the "requested party" should handle the case in the same manner as under the law of the "requesting party".

- Adoption of legislation to provide for mutual assistance to the "widest extent possible for investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense."



- In the absence of a mutual assistance treaty, the "requested party" may refuse if the request is considered to be a political offense or that execution of the request may likely risk its "sovereignty, security or other essential interest."

- Under the convention's requirements, countries are not obligated to consider dual-criminality when providing mutual assistance. In other words, if one country believes that a law under the convention's guidelines is broken and the perpetrator is in foreign territory, that foreign country, as the "requested nation", is required to assist the "requesting nation", regardless of whether the crime was committed in the "requested nation's" territory. The "requested nation" is allowed to refuse only if it believes the request is political in nature.[6]

Offences under the Convention:

Some of the offences under the convention include illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright and neighbouring rights.

It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production orders, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of trans-border access to stored computer data that does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the signatory parties. Further, as conditions and safeguards, the Convention requires the provision for adequate protection of human rights and liberties, including rights arising pursuant to obligations under the European Convention on Human Rights, the International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and shall incorporate the principle of proportionality.[7]

[6] Chapter 3 of the Convention
[7] Chapter 2 of the Convention

The Additional Protocol to the Convention on Cybercrime

In 2006, the Additional Protocol to the Convention on Cybercrime came into force. Those states that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivated by racism or xenophobia.

NIGERIAN CYBERCRIME LAWS VIS-À-VIS THE COUNCIL OF EUROPE CONVENTION

THE CYBERCRIMES (PROHIBITION, PREVENTION ETC.) ACT of 2015

Part VII of the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 mirrors the Council of Europe Convention, particularly with regards to international cooperation. The relevant sections are as follows:

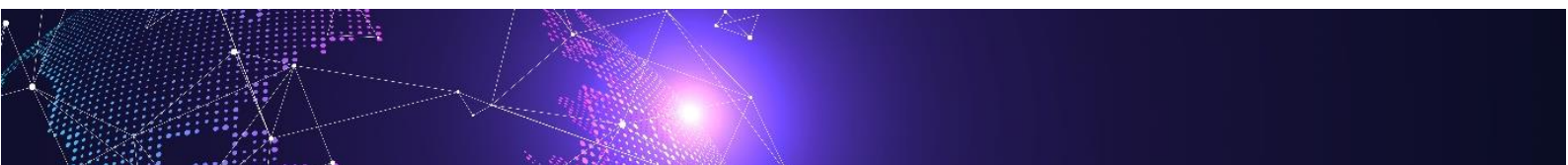
> "51. **Offences under this Act shall be extraditable under the Extradition Act, CAP E25, Laws of the Federation of Nigeria, 2004. Extradition.**
>
> 52. (1) **The Attorney - General of the Federation may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act.**
>
> (2) **The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country.**
>
> (3) **The Attorney-General of the Federation may, without prior request, forward to a competent authority of a foreign State, 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 under this Act.**

53. (1) Any evidence gathered, pursuant to a request under this Act, in any investigation or proceedings in the court of any foreign State, if authenticated, shall be prima facie admissible in any proceedings to which this Act applies.

(2) For the purpose of subsection (1) of this section, evidence is authenticated if it is –

(a) certified by a Judge or Magistrate or Notary Public of the foreign State; or
(b) sworn to under oath or affirmation of a witness or sealed with an official or public seal –
(i) of a Ministry or Department of the Government of the foreign State; or Evidence pursuant to a request.
(ii) in the case of a territory, protectorate or colony, of the person administering the Government of the foreign territory, protectorate or colony or a department of that territory, protectorate or colony."

Gleaning from the above provisions, it is pertinent for Nigeria to accede to international cybersecurity conventions as it has been demonstrated that cyber threats, unlike physical threats, are borderless and require the collaboration and cooperation of different states and actors in order to mitigate their devastating effects. Similarly, it is only through this cooperation and collaboration that the national laws on cybersecurity can have full effect. For example, section 52 of the Cybercrimes Act of 2015 mandates the Attorney General to request or receive assistance from any agency or authority of a foreign state in the investigation or prosecution of offences under the Act. Alongside the extradition provisions, these are not feasible unless Nigeria is seen to be cooperative and provides accession to the relevant conventions on cybersecurity, particularly the Council of Europe's Convention, which contains similar collaborative mandates.



THE RESPONSIBILITIES OF STAKEHOLDERS IN ACHIEVING CYBERSECURITY PROGRAMMES

Chapter 10 of the National Cybersecurity Policy and Strategy 2021 also outlines the need to enhance international cooperation. The chapter stands on a tripod stand, to wit:

a. Alignment of efforts of domestic cybersecurity stakeholders within Nigeria to enhance international engagement.

b. Strengthening cybersecurity influence on the regional stage.

c. Providing support for international mechanisms that promote cybersecurity

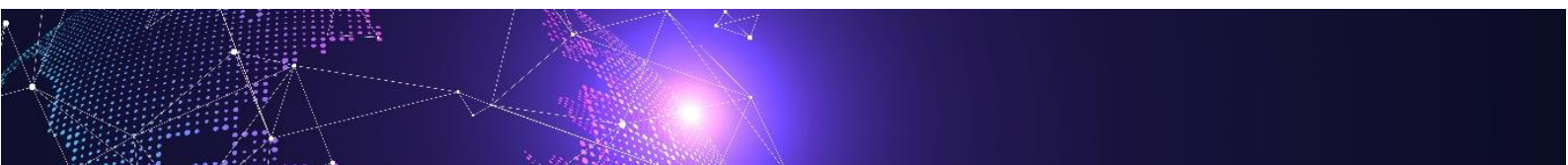
To achieve this, all hands must be on deck to ensure that our cyberspace is protected. To bring it to the fore, research has shown that as societies tend to move or tilt deeply into digital technologies, the more cybercrime we should be prepared to counter. In doing this, we need to leave no stone unturned, hence the importance of global cooperation in the warfare against cybersecurity threats.

Nationally, the Legislative Arm of government is saddled with the responsibility of developing and implementing comprehensive cybercrime legislation that is adaptable regionally and globally relevant in the context of securing the nation's cyberspace.

Through targeted awareness campaigns and advocacy, the Executive arm is responsible for increasing national awareness of cybersecurity and internet safety across all segments of Nigerian society.

The Judiciary, which includes Judicial Officers and Legal Enforcement Agencies, is responsible for improving their skills and competence in handling cybercrime cases.

Law enforcement agencies must also equip themselves, both human and infrastructure-wise, to prepare themselves for the wide range of sophisticated attacks that the country's cyberspace may face.



CONCLUSION

The need for a solid international framework cannot be overemphasized. Although we can say we have a comprehensive treaty on cybersecurity to which Nigeria has been invited to accede. It is clear that the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 captures some of the extant provisions of the treaty. It is important to point out that, it is more desirable not to be a lone ranger in the protection of our cyberspace.

We do hope that in the future, more steps will be taken to ensure that cyber security is in uniformity with international standards so that we can boast of robust symbiotic international cooperation, regionally and internationally.

According to Condoleezza Rice (former U.S. National Security Advisor), "*one thing that we can learn from the atomic age is that preparation, a clear desire and a clear willingness to confront the problem, and a clear willingness to show that you are prepared to confront the problem, is what keeps it from happening in the first place.*"

Contributor |

John Oladipo
Technology Law Group
john.oladipo@omaplex.com.ng