A COMPARATIVE ANALYSIS OF THE LEGAL FRAMEWORK FOR THE CRIMINALIZATION OF CYBERTERRORISM IN NIGERIA, ENGLAND AND THE UNITED STATES[*]

Abstract

Terrorism continues to pose a major threat to both national and international peace and security. It undermines the core values of the government. Nigeria continues to face multiple challenges posed by various terrorist groups with devastating human cost, in terms of lives lost or permanently altered, internally displaced persons and immensely negative consequences for economic and social development. Cyberterrorism is terrorism committed with the aid of a computer or computer network. This paper examines the provision which makes up the legal framework for the criminalization of cyberterrorism in Nigeria in comparison with that of England and the United States. The paper adopts a comparative legal method of analyses wherein the paper compares the legal framework in the different jurisdictions with the aim of interrogating the adequacy of the legislations. The paper further tries to assess and/or identify the gaps in the existing laws. The legal responses of both the national and international communities are analyzed in the paper. From the analysis, the paper finds that with the reoccurrence of terrorist attacks in Nigeria, the enactment of a law may not be enough, as cyber-terrorist attacks in Nigeria is imminent. The paper thereby recommends the establishment of a joint task force for cyber security and building of a National Cyber Command Center that will be the go-to center for cyber security in Nigeria and will facilitate Cyber intelligence integration for all governmental parastatals and other institutions in Nigeria.

Keywords: *Cyberterrorism, Terrorism, Security, Cyber-Security, Computer Network.*

1. Introduction

Information and communication technology (ICT) can be used to facilitate the commission of terrorist-related offences (a form of cyber-enabled terrorism) or can be the target of terrorists (a form of cyber-dependent terrorism). Specifically, ICT can be used to promote, support, facilitate, and/or engage in acts of terrorism. Particularly, the Internet can be used for terrorist purposes such as the spreading of propaganda (including recruitment, radicalization and incitement to terrorism); [terrorist] financing; [terrorist] training; planning [of terrorist attacks] (including through secret communication and open-source information); execution [of terrorist attacks]; and cyberattacks. Cyber-vector takes advantage of the structure of the Internet, which

[*] **ABIODUN ASHIRU; Graduate Assistant (LLM, LLB, B.L)** Department of Public and Private Law, Lagos State University, Lagos-Badagry Expressway, Ojo, ashiruabiodun@gmail.com.

enables computers around the world to communicate with each other *via* Internet Service Providers ("ISPs").

Computers or computer systems connected to the Internet through ISPs are assigned unique Internet Protocol ("IP") addresses, which may be dynamic (changing over time) or static. Computers communicate over the internet by contacting other computers, using the IP addresses of those other computers to identify them. Information is then exchanged between computers, identified by their IP addresses, *via* packets of information that are sent over the internet between the two devices. Shock and panic often face society with the strike of terrorist activities. The randomness and scale of attacks, causes great disbelief and outrage. The events of September 11 2001 clearly showed the global impact that an organized terrorist attack could have on various sectors. It also raised an awareness of the possibility of future attacks and the various repercussions. Although the attack was mainly a physical onslaught, the notion that computers and networks were used to orchestrate such an attack is raised. Cyber-attacks are an increasingly common nuisance but so far they have not been conducted by terrorists seeking to inflict the kind of damage that would qualify them as cyber terrorism by most definitions. This paper comprehensively examines the varying definitions of cyberterrorism while also examining the historical perspective, the dimensions, the legal responses (international, regional and local).

2. Conceptualizing Cyberterrorism

Cyberterrorism is terrorism and cyberspace combined. It is the unlawful attack and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.[1] Also, for an act to be termed cyberterrorism, it must have involved an attack that results in violence against persons or property, or at least cause enough harm to generate fear.[2] Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[3]

Cyberterrorism involves using computer network tools to shut down core national infrastructures (such as energy, transportation, government operations) or to force or belittle a government or civilian population. [4]The assumption about cyber terrorism is that as long as nations and critical infrastructure continue to depend more and more on computer networks for their operation, new vulnerabilities will continue to be created. [5]These vulnerabilities could be taken advantage of or exploited by a hostile nation or group and they can do this by penetrating

[1] D Denning. 'Cyberterrorism'. Available at http://www.Cs.Georgetoewn,edu/-Denning/Infosec/Cyberterror.html accessed on 25th May 2020.

[2] G Weimann. 'Cyberterrorism: How Real is the Threat?', United States Institute of Peace Special Report 119. Available at https://www.udsip.org/sites/default/files/sr119.pdf accessed on September 23. 2-320.

[3] D Denning, 'Cyberterrorism', available a<http://Www.Cs.Georgetown.Edu/~Denning/Infosec/Cyberterror.Html>, accessed May 25, 2020. See also D Denning, "Activism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy", available online at<http://Www.Cs.Georgetown.Edu/~Denning/Infosec/Nautilus.Html>>, accessed September 25, 2020.

[4] J A Lewis. 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats' *Centre for Strategic and International Studies* 2002, p. 209.

[5] *ibid*

a computer network that is not properly secured which would eventually disrupt or worse even shut down some very critical functions.[6]

Cyberterrorism is generally defined as an act of terrorism being committed through the use of cyberspace or computer resources. For instance, as simple as propaganda on the Internet that there might be a bomb attack at a specific time, such act can be termed cyber terrorism. Also, other acts that involve hacking directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.[7]Cyberterrorism is a high-speed and low-cost method of waging war that is within easy reach of poor countries, organizations and cells, giving them the capabilities to wreak tremendous damage on any nation attacked in this manner, particularly if the target is a computer-based industrialized nation. Two nations can have normal commercial and diplomatic relations, be at peace with each other and yet be simultaneously waging Cyber warfare against each other. One can attack the other's network systems from within its own territory or from other cybernetic platforms located in other countries or even continents. It is not a war waged in close-contact and the combatants don't know each other and possibly never will, but the damages caused can be quantified immediately. Cyber warfare and Cyber terrorism are a by-product and a vague aspect of globalization of economics, social activity, and trade and technology availability. For example, in the U.S., the number of people consulting the internet for health information online has grown from 54 million in 1998 to 160 million in 2007. In the case of U.S., by January 2007, 71% of all adults have gone online to look for specific health information.[8] Based on this analysis, Gordon and Ford are willing to counter the understandings of cyberterrorism that are farfetched, for example, the online purchase of airline tickets by the 9/11 attackers.[9]

2.2 Conceptual Clarifications

Cyberterrorism:

The term 'cyberterrorism' may be used to broadly classify unlawful activities relating to the terrorist use of the internet, or threats or actual malicious acts carried out either by physical or virtual means against computers, networks, or critical infrastructures with the intention to cause harm or to coerce a government or its people in furtherance of social, ideological, religious, or political objectives.[10]

Terrorism: The term 'terrorism' refers to criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political,

[6] J A. Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', (2002) *Center for Strategic and International Studies,* 21.

[7] D Denning; "Cyberterrorism, Testimony Before the Special Oversight Panel of Terrorism Committee on Armed Services", Us House of Representatives, May 23, 2000, available online at <http://Www.Cs.Georgetown.Edu/~Denning/Infosec/Cyberter Ror.Html>, accessed September 25, 2020.

[8] H Enghelberg, T*he Evolution of Cyber Terrorism A Precision-Delivery Weapon and the New Frontier In 21st Century Warfare* (Revised & Updated English Textbook Edition, London: Longman, 2012) 1.

[9] L Jarvis, L Nouri., and A Whiting., 'Understanding, Locating and Constructing Cyberterrorism', (2015) 9 (1) *Perspective on Terrorism,* 63.

[10] U J Orji, 'Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States', (2014) 6 (1) *Defence against Terrorism Review,* 33.

philosophical, ideological, racial, ethnic, and religious or any other nature that may be invoked to justify them. [11]

Cyberspace: The term 'cyberspace' is defined as the online world of computer networks and especially the internet.[12]

Cyberwarfare: The term 'cyberwarfare' has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.[13]

3. Brief Historical Evolution of Cyberterrorism

Cyber terrorism can be traced from June 1944 attack on the communication lines and logistic support of Germany. From 1945 the end of Second World War to 1991 the two super powers started to influence other nations through their dominant military force. It is known as cold war. The two 'super powers' were (1) the United States of America (USA) and (2) the Soviet Union.[14]

The conversation on cyber terrorism began in the late-1990s amidst a wave of high-profile terrorist attacks in the United States, including the bombing of the World Trade Center in 1993 and the Oklahoma bombing in 1995. By 1997, the US Department of Defense conducted its first ever no-notice information warfare exercise to test the cybersecurity of its own systems, and in the same year, the Marsh Commission report on critical infrastructure protection put the growing cyber threat landscape on the policy map in Washington.[15] Following the simultaneous bombings of the US embassies in Kenya and Tanzania in 1998 and the subsequent rise of al-Qaeda, terrorist attacks in and through cyberspace were seen as a potential future threat vector to the homeland. In October 1999, the Naval Post Graduate School prepared the first and to date most comprehensive study on 'cyber terror' for the US Defense Intelligence Agency.[16]

A 1999 study included numerous definitions and statements that outlined the contours of cyber terrorism research. The authors for example noted that "*terrorist use of information technology in their support activities does not qualify as cyberterrorism*." Similarly, they also excluded script kiddie techniques, including dictionary attacks, spoofed emails, and the bombardment of e-mail inboxes. Overall, the study narrowly defined cyber terrorism as "*the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies*

[11] The UN General Assembly Resolution 49/60 (adopted on December 9, 1994), titled "Measures to Eliminate International Terrorism".

[12] M Webster; 'What is Cyberspace?' *Merriam-Webster Dictionary*, available at <https://www.merriam-webster.com/dictionary/cyberspace>, accessed October 15, 2020.

[13] R A. Clarke and R A. Knacke, *Cyberwar: The Next Threat to National Security and What to do about it*, (Ecco; Reprint Edition, 2011) 25.

[14] M. Dasgupta, *Cyber Crime in India-A Comparative Study*, (Eastern Law House, Kolkata, 2009) pp. 191-193.

[15] Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection, October 1997, available online at <https://fas.org/sgp/library/pccip.pdf> accessed October 23, 2020.

[16] Naval Post Graduate School; 'Cyber Terrorism, Why it exists, Why It Doesn't, and Why It Will', available at <http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari47-2020-soesanto-cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will, accessed October 30, 2020.

in the pursuit of goals that are political, religious or ideological."[17] For a study compiled in 1999, this was a well-rounded framework. The only problem was that, in the United States, all cases that could theoretically fit the profile are statutorily considered either as acts that constitute cybercrime under the Computer Fraud and Abuse Act[18]or deemed armed attacks/acts of aggression under international law that would trigger the entire toolbox of US national defense mechanisms.

For the last 20 years, cyber terrorism researchers have unsuccessfully tried to carve out their own space that could stand apart from cybercrime, hacktivism, and offensive military cyber operations. It should thus not come as a surprise that, writing in 2012, Jonalan Brickey still had to explain that cyberterrorism could be defined as "*the use of cyber to commit terrorism*," or characterized as the *"use of cyber capabilities to conduct, enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change."*[19] Similarly in 2014, Daniel Cohen literally wrote a book chapter on 'cyber terrorism: case studies' in which all examples are either cases of hacktivism, cybercrime, or nation state operations.[20]

According to Hedi, we simply live and breathe today on the internet! We have become and probably are "slaves" to internet access, social media, smart phones and gadgets and we try to do almost all our activities *via* the internet maybe all our activities if we had the chance. Some years back, after the introduction of electronic voting by Venezuela which was as far back as 2004 adopted during their elections around 2004-2006, some other countries started to adopt the electronic voting method such that votes are being casted via the web or a tablet/smart phone.[21]

Explosives and guns are certainly not entirely analogous to computers. A better analogy might stem from the concept of an 'attractive nuisance'. For example, a homeowner shares some responsibility for injury caused by a pool on his property — it is deemed an attractive nuisance, and as such, the innocent should be prevented from simply being attracted and harmed. Thus, there are many instances of laws which already discuss damage done by/to a third party from the intentional/unintentional misuse of a piece of corporate/personal property. The application of these laws or the definition of 'misuse' with respect to computers seems unclear. However, there is a need for clear laws and standards which require operators of large networks of Internet-connected computers to exercise appropriate due diligence in their upkeep and security.[22]

4. Dimensions of Cyberterrorism

4.1 Computer Network Attack

Computer network attack (CNA): This includes any unauthorized access, or exceeding of one's access, to an information system that results in damage, enables potential future damage, or

[17] R T Berl 'Cyber terror: Prospects and Implications', A White Paper by the Center for the Study of Terrorism and Irregular Warfare Monterey, California, Prepared for Defense Intelligence Agency Office for Counterterrorism Analysis (TWC-1).
[18] 18 U.S.C. 1030
[19] J Brickey, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', *CTC Sentinel,* 2012, vol 5(8),p 6.
[20] D Cohen, 'Cyber Terrorism: Case Studies', in *Cyber Terrorism Investigator's Handbook*, Chapter 13.
[21] H Enghelberg, *The Evolution of Cyber Terrorism A Precision-Delivery Weapon and the New Frontier IN 21st Century Warfare* (Revised & Updated English Textbook Edition, 2012).
[22] Gordon Sarah & Ford Richard, Cyberterrorism? Symantec Security Response White Paper, 8.

allows for future unauthorized access to information, on any information system. Computer network attack is a broad term which tries to cover the complete range of malicious activity that a perpetrator may take against an information system. A computer network attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data.[23]

4.2 Electronic Attack (EA)

Electronic attack, most commonly referred to as an Electromagnetic Pulse (EMP), disrupts the reliability of electronic equipment through generating instantaneous high energy that overloads circuit boards, transistors, and other electronics.[24]EMP effects can penetrate computer facility walls where they can erase electronic memory, upset software, or permanently disable all electronic components.[25] Some military experts have stated that the few countries, including United States are perhaps the nation most vulnerable to electromagnetic pulse attack.[26]

4.3 Information System

Information system is an integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, and digital products. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. For instance, corporations use information systems to reach their potential customers with targeted messages over the Web, to process financial accounts, and to manage their human resources. Governments deploy information systems to provide services cost-effectively to citizens. Digital goods, such as electronic books and software, and online services, such as auctions and social networking, are delivered with information systems.

Individuals rely on information systems, generally Internet-based, for conducting much of their personal lives, for socializing, study, shopping, banking, and environment.[27]Cyber terrorists needs no internet access for committing the terrorist attack on the information structure, because latest attacks on Unites States using thumb drives, has proved it.[28] For security reasons, many critical infrastructure components and computers are deliberately not connected to the Internet as a safety and security reason, even though they remain vulnerable to cyber-attack.[29]

4.4 Cyber Attack

---

[23] *Ibid*, 9.

[24] HEMP Protection Systems, 'Maintenance of Mechanical and Electrical Equipment at Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (CCISR) Facilities,' *Army Training Manual* 5-692-2, April 15, Chapter 27, 2001. Available on <http://www.usace.army.mil/publications/armytm/tm5-692-2/chap27VOL-2.pdf> accessed November 3, 2020.

[25] K R. Timmerman, 'U.S. Threatened with EMP Attack,' Insight on the News, May 28, 2001, Available on http://www.insightmag.com/news/2001/05/28/InvestigativeReport/U.Threatened. With.Emp.Attack-210973.shtml, accessed November 3, 2020.

[26] S Schiesel, 'Taking Aim at An Enemy's Chips', *New York Times*, Feb. 20, 2003.

[27] V Zwass, 'Information System', available on <http://www.britannica.com /EBchecked/topic/ 287895/information-system>, accessed November13, 2020.

[28] K Zetter, 'The Return of the Worm that ate the Pentagon', *WIRED*, Dec. 9, 2011, Available on <http://www.wired.com/dangerroom/2011/12/worm-pentagon/>, accessed November 15, 2020.

[29] E Nakashima, 'Cyber-Intruder Sparks Massive Federal Response - and Debate over Dealing with Threats', *Wash. Post* (Dec. 9, 2011), Available on <http://www.washingtonpost.com/national/national-security/cyber-intruder-sparksresponsedebate/2011/12/06/gIQAxLuFgO_story.html>, accessed November 18, 2020.

A computer network attack, or cyber-attack, disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output. Computer hackers opportunistically scan the Internet looking for computer systems that are mis-configured or lacking necessary security software. Once infected with malicious code, a computer can be remotely controlled by a hacker who may, via the Internet, send commands to spy on the contents of that computer or attack and disrupt other computers.[30]

5. International Legal Responses to Cyberterrorism

The fast developments in the field of information technology have a direct bearing on all sections of modern society. The integration of telecommunication and information systems, enabling the storage and transmission, regardless of distance, of all kinds of communication opens a whole range of new possibilities. These developments were boosted by the emergence of information super-highways and networks, including the Internet, through which virtually anybody will be able to have access to any electronic information service irrespective of where in the world he is located. By connecting to communication and information services users create a kind of common space, called "cyber-space", which is used for legitimate purposes but may also be the subject of misuse.

These "cyberspace offences" are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The trans-border character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.[31]Concerned technical experts well understand that information security issues are inherently and unavoidably global in nature. Judicial and law enforcement officials equally well understand that the means available to investigate and prosecute crimes and terrorist acts committed against, or through the medium of, computers and computer networks are at present almost wholly local and national in scope.

The challenge therefore is how to regulate a technology that permits rapid transactions across continents and hemispheres using legal and investigative instruments that are fragmented across jealously but ineffectually guarded national and jurisdictional borders.[32]A growing number of states appear to have recognized that cybercrime and terrorism pose a significant threat to the infrastructure, commercial interests, and public policies of highly industrialized and highly computerized societies. This emerging recognition is reflected most directly in the national legal codes of concerned countries.[33]The problem however is how to use a national law to respond to an international problem. Hence, it is desirable to have an international response to cybercrime which occurs beyond the territory of one nation.

5.1 The Council of Europe Convention on Cybercrime

The **Council of Europe Convention on Cybercrime** also known as the **Budapest Convention on Cybercrime** or simply the **Budapest Convention** is the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative

[30] D Fulghum, 'Network Wars,' Aviation Week & Space Technology, Oct. 25, 200, 91,

[31] Paragraph 8 of the Council of Europe Convention on Cybercrime (The Budapest Convention) Explanatory Report.

[32] L Tonya L.; D Ellio; International *Responses on Cyber Crime*, (Hoover Press: Cyber, DP5 HPCYBE0200 06-25-:1 11:57:25 rev1) 36.

[33] The Budapest Convention and Related Standards, available at >https://www.coe.int/en/web/cybercrime/the-budapest-convention>, accessed November 30, 2020.

techniques and increasing cooperation among nations. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime, and as a framework for international cooperation between State Parties to this treaty.

The Convention is all out to pursue a common criminal policy against cybercrime. It promotes the harmonization of national laws, capacity building, and the fostering of international cooperation. It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states; Canada, Japan, Philippines, South Africa and the United States. The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of September 2019, 64 States have ratified the convention, while a further four states had signed the convention but not ratified it.[34] Since it entered into force, important countries like Brazil and India have declined to adopt the Convention on the grounds that they did not participate in its drafting. Russia opposes the Convention, stating that adoption would violate Russian sovereignty, and has usually refused to cooperate in law enforcement investigations relating to cybercrime. It is the first multilateral legally binding instrument to regulate cybercrime.[35]

The Budapest Convention is a criminal justice treaty with a specific focus on cybercrime and electronic evidence. It requires Parties (a) to criminalize a range of offences against and by means of computers, (b) to provide criminal justice authorities with procedural powers to secure electronic evidence in relation to any crime and (c) to engage in efficient international cooperation. The first pillar on substantive criminal law covers in Articles 2 to 11, offences against (i) the confidentiality, integrity and availability of computer data and systems, (ii) computer-related offences, (iii) content-related offences and (iv) offences related to infringements of copyright and related rights. In the separate *Additional Protocol to the Convention on Cybercrime*, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems ("Additional Protocol"), certain offences related to acts of a racist and xenophobic nature are dealt with.

The second pillar is a set of specific procedural provisions that describe in detail the powers that criminal justice authorities may exercise when investigating the criminal offences against and by means of computers established under the first pillar, but also when investigating any other offences where evidence may be found on computer systems. These powers must be subject to conditions and safeguards to protect the rights of individuals. In this respect, the *Budapest Convention* is not just a cybercrime convention but one that also provides the basis for collection of electronic evidence relating to other crimes, such as murder, terrorism, drug trafficking and other serious crime. Hence, it is effectively a convention on both cybercrime and electronic evidence.

The third pillar is an extension of the second pillar into the international arena, providing a mechanism for international cooperation in matters not only related to cybercrime but again to police to police and judicial cooperation in relation to any crime involving electronic evidence. The *Budapest Convention* is backed up the Cybercrime Convention Committee, which among

[34] Council of Europe 'The Budapest Convention and Related Standards' available vat https://www.coe.int/en/web accessed on 09/26/2021.

[35] J Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization', *Monash University Law Review*, 2014, vol 40(3) p.700.

other things, assesses implementation of this treaty by the Parties, and by capacity building programmes. The Budapest Convention thus, provides a comprehensive, operational and functional solution for the investigation and prosecution of cybercrime both domestically and between Parties, with a global reach.[36]The Convention did not expressly make provision for the offence of cyberterrorism as one of the offences punishable under it. However, the Convention requires state parties to adopt in their domestic laws measures to prohibit and punish illegal access to computers for the purpose of infringing on their securities. This invariably has dealt with the offence of cyberterrorism since the concern of this offence is basically to protect the security and welfare of the citizens.

5.2 The African Union Convention on Cyber Security and Data Protection

The *African Union Convention on Cyber Security and Data Protection* also known as the *Malabo Convention* is a Convention adopted by the African Union in response to the concerns of cyber insecurity in Africa. Ministers in charge of communications and Information technologies adopted a declaration[37]in which they requested the African Union Commission to develop jointly with the United Nations Economic Commission for Africa, a convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection." This Declaration has been endorsed by the 14th AU Summit of Head of State and government in 2010[38]and confirmed again by the third ordinary conference of Ministers in charge of ICT held in Abuja in August 2010 in their declaration.[39]

The AU Convention represents a political commitment by African States to take measures on a range of issues, including cybercrime and basically aims to harmonize the laws of African States on electronic commerce, data protection, cybersecurity governance and cybercrime control. The Convention also defines the objectives for the information society in Africa and seeks to strengthen existing ICT laws in Member States and the Regional Economic Communities (RECs).[40]The Convention requires Member States to promote cyber stability by establishing appropriate cybersecurity governance frameworks. In this regard, Member States are required to establish a national cybersecurity framework that comprises a national cybersecurity policy and a national cybersecurity strategy.[41]

Article 26 of the Convention establishes obligations on Member States to promote a culture of cybersecurity amongst all stakeholders (such as governmental institutions, businesses and the civil society) that develop, operate, or use information systems and networks while Article 25 of the Convention imposes obligations on Member States to establish appropriate structures or institutions as well as regulatory powers that are necessary for cybersecurity governance.[42]The Convention imposes obligations on Member States to criminalize substantive criminal acts that affect the confidentiality, integrity, availability and survival of ICT systems, and the data

[36] Z Jamil, 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime', (Global Action on Cybercrime Extended, Glacy, Version 20, 2016), 3. Also available online at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bf0f8>, accessed November 30, 2020.
[37] [EXT/CITMC/MIN/Decl. (I)] (Olivier Tambo Declaration) 2009.
[38] [Assembly/AU/11(XIV)]
[39] ([AU/CITMC/MIN/Decl.(III)].
[40] Preamble to the AU Convention on Cybersecurity and Personal Data Protection, 2014.
[41] *Ibid*, Article 24.
[42] *Ibid*, Article 25:2.

processed by such systems. This implies that Member States are required to establish offences that criminalize acts such as unauthorized access to a computer system, unauthorized interference with a computer system or data, and unauthorized interception of data processed by a computer system. In addition, the Convention requires Member States to criminalize substantive criminal acts that affect ICT network infrastructure.[43]

Till date, the Convention is not in force. The Convention will enter into force after it has been ratified by 15 AU Member States. According to a report by the AU, as of May 2018, only 10 AU Member States (Benin, Chad, Comoros, Congo, Ghana, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia) had signed the Convention, while two Member States (Mauritius and Senegal) had ratified the Convention. As of June 2020, 8 AU Member States have ratified the Convention while 14 Members have signed the document.[44] The whole chapter III of the Convention comprising of Articles 24 to 31 deals with Cybercrime. The Convention requires the state parties to adopt within their national legislations measures to protect their security including cybersecurity.

5.3 Comparing the Council of Europe Convention on Cybercrime and the African Union Convention on Cyber Security and Data Protection.

The AU Convention is, on the one hand, broader than the Budapest Convention in that it covers Electronic transactions, Personal data protection and, Cyber security and cybercrime Thus, the AU Convention is an attempt to unite different aspects related to information technology law and certain non-digital and non-criminal justice issues. On the other hand, the Budapest Convention's scope is limited to cybercrime as the law makes only provisions for cybercrime and cyber criminality. However, with regard to cybercrime and electronic evidence, the AU Convention criminalizes some but not all of the conduct foreseen under the Budapest Convention.

Moreover, the AU Convention does not provide for the full set of procedural powers for investigating and prosecuting cybercrime and securing electronic evidence in domestic investigations. And finally, the AU Convention does not contain specific provisions and does not constitute a legal basis for international cooperation on cybercrime and electronic evidence.[45]

The AU Convention represents a political commitment by African States to take measures on a range of issues, including cybercrime. The AU Convention contains, in some form, the offences of the Budapest Convention. Several of the offences, in particular the provisions corresponding to electronic fraud and electronic forgery and content-related offences such as child pornography and offences related to xenophobia and racism are covered by the AU Convention and are largely consistent with the Budapest Convention. Moreover, certain high-level principles within the AU Convention appear to match various articles of the Budapest Convention.[46]In that sense, in principle, the Budapest Convention and the AU Convention appear to have a degree of compatibility.

---

[43] *Ibid*, Article 25:1.

[44] List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection, available online at <https://au.int/sites/default/files/treaties/29560-sl-african%20union%20convention%20on%20cyber%20security%20and%20personal%20data%20protection.pdf>.

[45] AU Convention *supra* note 34.

[46] Draft AU Convention in fact specifically mentioned the Budapest Convention in the following terms: "Article III(1)(1) – Member States shall take into account the approved language choice in international

6. A Comparative Analysis of the Legal Framework for the Criminalization of Cyberterrorism in Nigeria, England and the United States.

As Computer-fraud crimes prevailed, especially the *Advance Fee Fraud* also known as *'419'* or *'Yahoo Yahoo'*, the Nigerian youths used this as a medium of collecting money from unsuspecting Nigerians by impersonating government officials or companies well known to people to avoid any form of suspicion. The commission of this offence was possible as there were no laws in Nigeria to combat computer crimes and this led to the ideal environment for criminals to freely operate without the fear of prosecution. After all, a Nigerian citizen cannot be punished for an offence unless such offence was codified in a written law and the punishment prescribed thereafter.[47]The Cybercrime (Prohibition, Prevention, etc.) Act (hereinafter 'the Cybercrime Act') is the principal legislation on cybercrime in Nigeria. This piece of legislation was enacted for the prohibition, prevention, detection, prosecution and response to cybercrime and other related offences.

Section 18 of the Cybercrime Act creates and punishes the offence of cyberterrorism. The section makes it an offence to access any computer or computer system for the purpose of terrorism. The section provides that "any person that accesses or causes to be accessed any computer or computer system or network for the purposes of terrorism commits an offence and is liable on conviction to life imprisonment.[48]It is assumed the purpose of the provision of section 18(1)is, however, to prevent access to government computers, computer systems, or networks or any computers, computer systems, or networks used for public functions or sensitive purposes without right or authorization - which may be a first step in perpetrating cyber-attacks.

The second level is the launching of an attack that can be regarded as act of terrorism which has been stated in section 18(2) as having the same meaning under the Terrorism (Prevention) Act, 2011(as amended in 2013).[49]This signifies that the provisions of section 18 of the Cybercrime Act should be read in conjunction with the Terrorism (Prevention) Act. It should be noted that "terrorism" itself does not have precise definition under the Terrorism (Prevention) Act but the scope of proscribed acts of terrorism is provided for under section 1(3) of the Act. Under the Cybercrime Act, cyberterrorism must target the information or critical infrastructure through the cyberspace to be so qualified, and must carry with it as required under section 18(2) of the Cybercrime Act the consequences listed as terrorism acts under section 1(3) of the Terrorism (Prevention) Act.

In England, the Computer Misuse Act (CMA) 1990 is a key piece of legislation that criminalizes the act of accessing or modifying data stored on a computer system without appropriate consent or permission. It was devised after the *Regina v Gold and Schifreen* case,[50]in which two hackers remotely accessed BT's Prestel service at a trade show using the credentials of a BT engineer. The idea of a Computer Misuse Act was first proposed at a time when computers were a rarity in public life. Under its initial iteration, what was

cybercrime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations where necessary."

[47] Constitution of the Federal Republic of Nigeria 1999, s.36 (12); See also the case of *Aoko v Fagbemi* (1961) All N.L.R. 400.

[48] Cybercrime (Prohibition, Prevention etc.) Act 2015, s.18 (1).

[49] *Ibid*, s18 (2).

[50] [1988] 1 AC 1063 (HL).

considered a malicious act was quite narrowly defined, largely because the ways in which you could cause harm were also fairly limited. However, the rise of the digital age over the past 20 years has meant the act has been reshaped to respond to a growing variety of threats and potential avenues for harm. That not only includes the various attack methods that criminals can now deploy, but also the act of preparing for an attack is now considered malicious.

The CMA did not specifically criminalize cyberterrorism unlike the Nigerian Cybercrime Act. However, a holistic reading of section 1 of the Terrorism Act reveals that cyberterrorism is criminalized in England.[51]The Act defines 'cyberterrorism' as the use of violence or threat of action which is designed to interfere with or disrupt through electronic system the government or to intimidate the public or a section of the public.[52]The penalties for terrorism under the CMA varies depending on the form of terrorist activities which the accused person was involved in. For instance, the culpability of a person who shows his support publicly for a terrorist organization is not exceeding ten years while a person who wears the uniform to a terrorist group in public will be liable to an imprisonment term not exceeding 6 months imprisonment.[53]

The United States founded the Internet and leads the world in terms of Information and Communication Technology even though it is a prime target of both physical and online terrorist attacks. Following the 9/11 attacks, the anti-terrorism legislation, the 'USA PATRIOT Act'[54]was passed by the US Congress and endorsed by George W. Bush, the 43rd President of the United States, in 2001. This legislation is intended to empower the US law enforcement authorities to fight terrorism both on US soil and overseas with regard to cyber terrorism, Section 814 of the Act 'Deterrence and Prevention of Cyberterrorism' amends a pre-existing computer crime related provision, Section 1030 (a)(5) of title 18 of United States Code (Computer Fraud and Abuse Act) According to the amended section, a person commits an offence of cyber terrorism if he/she:

> **(a)** knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> **(b)** Intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
> **(c)** Intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage.[55]

Also, as an additional requirement of this section, criminal conducts stated above must cause:

(i) Loss to one or more persons during any one-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000 in value.

[51] The United Kingdom Terrorism Act 2000, s1. This provision deals with the interpretation of terrorism.
[52] This definition is reached from a combined reading of Section 1 (1) a and (2) e of the Terrorism Act 2000.
[53] The Terrorism Act sections 12 and 13 respectively.
[54] The 'USA Patriot Act' Stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.
[55] Section 1030 (A) (5)(A).

(ii) The amendment or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.
(iii) Physical injury to any person.
(iv) A threat to public health or safety; or
(v) Damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. A person accused of the violation of this provision is punishable by a fine or life imprisonment.

It can be said that the 2001 Act was passed to strengthen the punishment of particular computer crime-related activities which have the potential to cause harm to national security, economy and welfare. In other words, it was the legislated for the sole aim of combating cyber terrorism. Among the laws analyzed above, it is evident that the American legal framework contains a more comprehensive provision on the subject, 'cyberterrorism'. One of the shortcomings of the Nigerian provision on the subject is that the Cybercrime Act relies on the provision of the Terrorism Prevention Act for the definition of terrorism. The latter of which did not in itself define the term 'terrorism'. Prosecution on this provision may not likely succeed since there is no definitive definition of the scope of the offence. In England however, cyberterrorism is not specifically criminalized. The provision relied on to criminalize the act is the definition given by the Terrorism Act. This provision may not be reliable in its entirety as there exists under the latter various acts and omissions which may lead to terrorism with varying culpabilities and punishment. This may in turn make it difficult for the prosecution to bring a charge under the appropriate heading.

7. Conclusion

It is more than obvious that the way of conducting terrorism with the time is becoming more sophisticated.

Terrorism has entered a new wave in that the latest battleground to emerge is cyberspace. The potential threat posed by cyberterrorism has provoked considerable alarm.

Numerous security experts, politicians, and others have publicized the danger of cyberterrorists hacking into government and private computer systems and crippling the military, financial, and service sectors of advanced economies.

Cyberterrorism is the latest catchphrase in the domain of cyber-attacks, cyber-crime and network warfare. Cyberterrorism has become a realistic threat in that those seeking to damage/disrupt computer systems, programs, infrastructure and data, could leave a meaningful impact on the civilian sector. This paper has examined the definitions, the techniques and the legal responses to cyberterrorism.

8. Recommendations

This paper recommends as follows:
A joint task force for cyber security should be established in Nigeria.

In addition, there should be building of a National Cyber Command Center that will be the go-to center for cyber security in Nigeria. This will undoubtedly facilitate cyber intelligence integration for all governmental parastatals and other institutions in Nigeria is desirable.

It is also recommended that there is a need to have Judges and Law Enforcement Officers that are technically and technologically sound in understanding cybercrime and its terminologies, appropriately interpreting the law on cybercrimes and keeping up with the trends of cyber environment.

Further, it is desirable to have local and international collaboration between private, governmental and civil society in intelligence and data sharing and other international treaties on cyber security.