International Journal of Innovative Legal & Political Studies 8(3):25-36, July-Sept., 2020

© SEAHI PUBLICATIONS, 2020 www.seahipaj.org ISSN: 2467-8503

Cyberterrorism and the Protection of Critical Information Infrastructure in Nigeria: A Legal Assessment

Dr. Nuleera A. Duson* & Sunny D. James**

ABSTRACT

The well-being of any nation depends upon secure and resilient critical infrastructure. Government business can be brought to a halt if critical information infrastructures are attacked. Similarly, many private businesses may also grind to a halt if critical information infrastructures are attacked. Critical infrastructure refers to the various systems, networks, facilities and services upon which the daily life of a nation depends. One of such infrastructure is the power network that provides the nation with electricity. A major attack on a nation's power grid would shut down any country. The advent of cyber as a weapon of warfare is rapidly gaining momentum the world over and Nigeria is not immune to such threats. In 2012, it was reported that there was about 60 percent increase in the attacks on Nigerian Government websites. This paper examines the concept of cyber-terrorism and the possibility of terrorist organizations like the Boko Haram sect using the cyber to perpetrate terrorist acts in Nigeria. The paper argues that the Cybercrimes (Prohibition, prevention) Act 2015, in its current state cannot adequately address the issue of cyber-terrorism and the protection of critical national infrastructure in Nigeria. The law does not provide for a single enforcement institution and as such the enforcement framework is chaotic. This paper suggest an amendment to the Act and to include the creation of a cyber attack prevention agency that will be saddled with enforcement of the Act and developing the technical capacity of local technocrats to be able to manage the cyber security risks to Government and private sector critical information infrastructure. The paper also recommend the need for Nigeria to sign and ratify the convention on cybercrime which came into effect on 1 July 2004 and the Global Security Agenda (GSA) launched by the International Telecommunication Union in May 2007 in addition to adoption of other deliberate polices and measures to safeguard national critical infrastructures and more importantly save lives' for as cyber-terrorism is a combination of an urge to cause terror mixed with technological advancements, no single measure can successfully combat it.

Keywords: Cyber-terrorism, Cybercrimes, Critical Information Infrastructure, Protection.

1. INTRODUCTION

Information technology provided an impetus to the growth of e-commerce and assisted in rapid transmission of information and communication.[1]However, the IT age has also germinated multifarious cybercrimes such as phising, hacking, cyberporn, cyber-terrorism and cyber contraventions such as network system damage, disruption of computer systems or blocking access to another authorized user and time thefts.[2] With the advent of computer, the internet and various technological innovations, there arose monstrous criminal and antisocial activities perpetrated by criminals. The growing dependence of societies today on ICT has open a window form of vulnerability, giving terrorists the opportunity to approach targets that would otherwise be utterly assailable such as national defence system and air traffic

* PhD (Nigeria), BL, Lecturer, Department of Law, Institute of Legal and Global Studies, Captain Elechi Amadi Polytechnic, Port Harcourt, Email of the corresponding author: drnuleera@gmail.com .,08035525300.

**BSC (Pol. SC.) (Uniport) LLM. (RSU) BL,. Lecturer Department of Law, Institute of Legal and Global Studies, Captain Elechi Amadi Polytechnic, Port Harcourt, PhD Research Fellow, Faculty of Law, Rivers State University,

[1]K. Seth., Cyber laws in the information Age, Lexis Nexis Butherworths Wadhwa, Nagpur, India, 1st edn., 2009, P.437

[2] Ibid

control system.[3] The more technologically developed a country is, the more vulnerable it becomes to cyber attacks against its infrastructures.[4]

Addressing the terrorism phenomenon is a very complex and challenging task[5] while condemnation of terrorist activities by the international community has been unanimous and unequivocal, efforts to regulate this phenomenon have been marred by differences of approach and competing concerns.[6] The role of computer with respect to terrorism is that of modern thief who can steal more with a computer than with a gun.[7] The terrorist may be able to do more damage with a keyboard than with a bomb.[8] The tremendous role of computers in our daily life has stimulated criminals and terrorists to make it their preferred tool for attacking their targets.[9] The internet has provided a virtual battlefield for countries having problems with each other such as Taiwan against China, Israel against Palestine, India against Pakistan, China against United States and many other countries.[10]

This transformation in the methods of terrorism from traditional methods to electronic methods is one of the biggest challenges to modern societies.[11] The challenge facing the international community is translating the statements and well elaborated declarations of condemnation of terrorism into concrete measures (Legal, Political, and Military) that can effectively address the very negative effects and consequences of terrorist activities.[12] Nigeria is not an exception as the Boko Haram sect poses a very big threat to the survival of the nation. The tendency of the sect resorting to cyber-terrorism is very real and there is the dare need to safeguard critical infrastructures and the citizens through effective legislations and policies. The focus of this paper is on the concept of cyber-terrorism, the possibility of groups like Boko Haram sect using it to attack critical national infrastructures in Nigeria and to ascertain whether the cybercrimes (Prohibition, Prevention) Act 2015 is adequate to combat the menace.

2. The Concept of Cyber-terrorism

The concept of cyber-terrorism cannot be discussed in isolation without understanding the concept of terrorism.[13] The concept of cyber-terrorism does not on itself stand alone, without first understanding the meaning of terrorism.[14] The Concept of terrorism has not been easy to define in a manner that is universally acceptable. According to Schmid,[15] between 1936 and 1981, 109 definitions of terrorism have been offered. The reason for the difficulty in finding an acceptable definition of terrorism is because defining terrorism is a moral problem.[16] This moral factor was also responsible for the failure in the 1970s by the UN to adopt a universal convention on Terrorism.[17] Two weeks before the opening of the 27th session of the UN General Assembly in September 1972, the subject of international terrorism was trust upon the consciousness of the world community by the murder of 11 Israeli athletes at the Olympic village in Munich. Shocked by the Munich Massacre, the then Secretary General, Kurt Waldheim proposed an item in the agenda for measures to prevent terrorism and other forms of violence which

---

[3] G. Weimann, Cyberterrorism: How real is the threat? United States Institute for Peace, Special Report 119, December 2004, P. 2

[4] Ibid.

[5] R.K Chanbey., An introduction to cybercrime and cyberlaw, Kamal Law House, Kolkata, India, 2nd edn. 2008, P. 472

[6] Ibid.

[7] Ibid.

[8] Ibid

[9] Ibid. P. 474

[10] Ibid

[11] Ibid

[12] Ibid. P. 472

[13] M. Devost and N. Pollard., 'Taking Cyber-terrorism seriously-failing to adapt to threats could have dire consequences' (2002), Available at < https://www. terrorism.com > accessed 2/6/2020.

[14] C.R. Ibekwe., 'Cyber-Terrorism offences under the Nigerian Legal system', in F.E. Eboibi(ed), Hand book on Nigerian Cybercrime Law, (Justice Jeco printing and publishing Global 2018), P.414.

[15] A. Schmid., Political Terrorism: A research guide, (London, Sweet & Maxwell 1993)

[16] I. Okoronye., Terrorism in International Law, (Whytem, Publishers Nigeria, 2013), P.13

[17] Ibid

endanger…human lives or Jeopardize fundamental freedoms.[18] The item was approved by the General Committee but seven negative votes were cast against it by Asian and African countries. According to Libya, Syria and Mauritania with the active support of Guinea, Mauritius and China, the inclusion of the item, would constitute yet another attempt to classify the legitimate struggle of people under the yoke of Colonialism and alien domination as 'terrorism'.[19] Be that as it may, Terrorism has been defined as the threat of violence, individual acts of violence, or a campaign of violence designed primarily to instill fear to terrorize.[20] The League of Nations convention for the prevention and punishment of terrorism 1937 posits that acts of terrorism are criminal acts directed against a state or intended to create a state of terror in the minds of particular persons or group of persons or the general public.[2]The United Nations Resolution 1566, defines terrorism as:

> Criminal acts including against civilians, Committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.[22]

The Resolution calls upon all states to prevent such acts and, if not prevented to ensure that such acts are punished by penalties consistent with their grave nature.[23] In the case of ***Karimu* v. *Federal Republic of Nigeria,*[24] NIMPAR JCA,** held that:

> Terrorism is a serious offence and its effect is beyond the offence of just killing one human being. The effects of terrorism include injuries, death, psychological trauma of the immediate victims. It has short and long terms effects on the society and nation. It also impacts on the economy of the entire nation. Buildings and infrastructure are damaged. It has no classified enemy except total destruction. Life is reduced to an imaginable state of no value. It is a notorious fact that lives are wasted by the mere acts of some demented individuals who have made themselves outlaws. No society would sit back and tolerate such acts. Infact, terrorism has no defined enemy except the general destruction of human lives and livelihood. It is not a conventional fight or agitation. It is a fact that thousands of lives have been wasted in a region of this country, innocent citizens displaced from their ancestral homes as a result of various acts of the proscribed Boko Haram group. The Appellant and his friends travelled all the way from the North-East where terrorism has become prevalent, to Lagos and commenced preparations to introduce their callous act of total destruction of innocent lives for just no reason. Lagos is a densely populated city and if not for the timeous action of the security agencies, the story would have been different today. Besides, the victims could have been anybody.[25]

Similarly, cyber-terrorism is a term esoteric, complex and difficult to circumscribe within the four corners of a definition which will be universally acceptable.[26] While the word 'Cyber' relates to

---

[18] S. M. Finger, 'The United Nations Response to Terrorism' in Alexander Y and R. Kilmaxx (eds), Political Terrorism and Business: The Threat and Response, (New York, Praeger Pub. 1979), P. 260

[19] Ibid.

[20] B. Jerkins., International Terrorism: A New code of conflict, (Los Angeles, Crescent Publishers 1975), P.1.

[21] League of Nations convention for the prevention and punishment of Terrorism 1937. The convention never entered into force because of the onset of the Second World War.

[22] UN Resolution 1566, of 2004. Available at < https:// daccessdds. Un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282. pdf? Open Element > accessed 6/6/2020.

[23] Ibid.

[24] (2017) All FWLR (Pt 898) at pp.190-191, Paras. F-C, P.192

[25]Ibid.

[26] T. Fatima., Cybercrime, (Eastern Book Company, 2011), P.196.

cybernetics, which is a tool of trade, 'terrorism' denotes an act of violence.[27] The ambiguity in the definition of the term cyber-terrorism brings indistinctiveness in action as Dorathy Denning points out, 'An email may be considered hacktivism by some and cyber-terrorism by others.[28] The term cyber-terrorism was coined in 1997 by Barry Collin, a Senior Research fellow, institute for security and intelligence, California.[29] He defined cyber-terrorism as the convergence of cybernetics and terrorism.[30]In the words of Kelvin Coleman,[31] Cyber-terrorism is the premeditated use of disruptive activities or the threats thereof against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives. The Federal Bureau of Investigation posits that cyber-terrorism is premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against non-combatant targets by sub-national groups or clandestine agents.[32] The U.S National Infrastructure protection centre opined that cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence destruction and/or disruption of services to create fear by causing confusion and uncertainly within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda.[33] Terrorism experts, Dorathy Denning defines Cyber Terrorism as unlawful attacks and threats of attacks against computers and networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political and social objectives.[34]

Dorathy Dennings definition of Cyber-terrorism consists of several important components. First, it portrays the fact that the attack should be unlawful; secondly, the attack and threats of attacks should be directed against computer, networks and/or the information stored within them; thirdly, the purpose of these unlawful attacks is to intimidate or influence a government or society to further their political or social objectives, fourthly, the attacks must result in violence against members of the state or their property or at least cause enough harm to generate fear amongst the citizenry and finally, that serious attacks against critical infrastructure could be construed as acts of Cyber-terrorism depending on their impact.[35]Cyber-terrorism has several distinct characteristic.[36] These characteristics help to better differentiate between a cyber-terror and a mere attack or activities of a hacker. According to Chanbey, Cyber-terrorism will and may display the following signs.[37]

a. Attack is predefined and victims are specifically targeted.
b. Attack has an objective to destroy or damage specific targets such as political economic, energy, civil and military infrastructures
c. Attack may even target specific opposing religious group's information infrastructures to insight religious pandemonium
d. The purpose of any attack is to create fear of the group's intentions and further their own political agenda or goals or gain fellowship by succeeding in their attacks.

---

[27] Ibid.
[28] D. Denning, 'Activism, Hacktivism and Cyber-terrorism: The internet as a tool for influencing Foreign Policy'. Available at < https://www.nautilis.org/info-policy/workshop/papers/denning.html > accessed 3/5/2020.
[29] B.C. Collin, 'The future of Cyber-terrorism' proceedings of the 11th Annual International Symposium on criminal Justice issues, the university of Illinois at Chicago, 1996
[30] Ibid.
[31] K. Coleman, Cyber Terrorism, Technolytics, October 10, 2003.
[32] The Federal Bureau of Investigation (FBI), is the Primary investigative arm of the United States Department of Justice (DOJ). See FB1 quick facts. Available at < https://www.fb1.gov/quickfacts.htm > Accessed 3/5/2020.
[33] The National Infrastructure Protection Centre (NIPC) is charged with assessing threats to critical infrastructure, particularly computer systems and providing warnings concerning threats and vulnerabilities. It also conducts investigations and provides a response to computer attacks.
[34] D. Denning 'Cyber Terrorism, Testimony before the special oversight panel on Terrorism committee in Armed services, US House of Representations by Georgetown University' (23-5-2000), Available at https://www.cs.georgetown.edu/denning/infosee/cyberterror.html > Accessed 6/6/2020 .
[35] G. Weimann., 'Cyber-terrorism', 2004.
[36] R. K. Chanbey, (n5) P. 479
[37] Ibid.

e. Destroy the enemy's capabilities to further operate within their own arena.
f. Persuade others to believe that the victim or victims are vulnerable and their stability negligent.
g. Create increased loyalty and pride within the group based on their successes

The methods used by cyber-terrorists thrive on the development of new technologies.[38] Although often developed for some other non-threatening purpose, new technological advancements provide terrorists and cyber-terrorists with new weapons for their arsenal.[39] These new weapons include: Radio frequency weapons.[40] Transient Electromagnetic Device (TED).[41]RF, munitions,[42] Tempest monitoring devices,[43] Electromagnetic bombs,[44] and computer viruses and other related harmful computer programs. Interest in these new technologies has been substantially increased by the widespread availability on the internet. Several serious dangers are presented by many of these new weapons. They may allow the user to attack from a great distance (a computer terminal thousands of miles away from the target, for example); the attack is undetectable and a victim may not even know that he is being attacked; and there are no protective measures currently available to protect a potential target from attack.[45] The internet provides a means for easy communication between two or more parties, communication that might not be traceable as point to point communication as in a telephone call. The terrorist also adopt steganography. This is a process of hiding information in objects such as photos, other documents and other type of files.[46] If encryption, drop sites and steganography are combined, the communication of terrorist will be hard to detect. [47]Computers can be embedded within destructive devices to make their deployment, control and timing much more precise and difficult to detect and disarm.[48]Computers also provide the ability for multiple devices to communicate autonomously.[49]This means that more sophisticated terrorist bombs are on the horizon.[50] One fact which is in favour of the cyber-terrorists is that no field is moving as quickly as computer and communication technology which forms the basis for cyber-terrorism.[51]Cyber-terrorism is a transformed strategy and an attractive alternative to terrorist in perpetrating their acts. Terrorist prefer the use of cyberspace in achieving their targets. It proves to be cheaper and easier than the traditional terrorist methods. What the terrorist needs is a personal computer and online connection. Cyber terrorism further conceals the identity of the terrorist. The terrorist need not to buy guns, weapons and explosives, instead they create and deliver computer virus through wireless connection, cable and telephone lines, cyber-terrorism or other forms of disclosure and this have made it easier for terrorist organizations to recruit and retain followers.

[38] Ibid. P. 484
[38] Ibid.
[39]These devices typically consist of a power source, an apparatus to generate RF energy, and antennae to direct the energy. The RF waves created by the weapons are similar to FM radio waves. The RF weapons emit a series of smooth radio waves that cause the targeted material or device to generate heat and burn up.
[41] The TED has been referred to as the weapon of choice of the modern cyber or infrastructure RF warrior. A special category of RF weapon, the TED emits a large 'spike' burst of energy as opposed to a series of waves.
[42] RF weapons may be converted into deliverable munitions such as hand grenades, mortar rounds, or artillery shells.
[43] Ibid.
[44] The electromagnetic bomb creates an electromagnetic pulse which is an electromagnetic shock wave. The damage inflicted upon the target by this shock is similar to the damage that would be inflicted by a lightning strike.
[45]See Verton., Dan Black Ice; The invisible threat of cyber-terrorism. Osborne/Mc Graw-HiD, U.S 2003.
[46]R. K. Chanbey, (n5) P. 483.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] See Spydes., Jimmy & Byars, will 'Examples of cyber-terrorism'.
[51] R. K. Chanbey., (n5) P. 485
[52]M.Gerke., 'Understanding cybercrime: A guide for Developing countries (TTU 2009)'Available at < https://www.itu.in/ITU-D/cyb/cyersecurity/legislation/html > Accessed 3/6/2020.

3. Critical Infrastructure Vulnerability

Terrorists can use Information Communication Technologies (ICTs) and the internet for different purposes: Propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, terrorist financing and attacks against Critical Infrastructures.[52] What this means is that organizations or governments which depend on the operation of computers and computer networks can be easily attacked. Each single form of malicious cyber activity has internet potentials to attack critical infrastructure. Critical Infrastructure are assets, systems and networks, whether physical or virtual, so vital to a state that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.[53] Critical Infrastructure means, systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country.[54] Critical National Information Infrastructure are those assets, systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on:

1) National economic strength; confidence that the nation's key growth area can successfully compete in global market while maintaining favourable standards of living;
2) National image; projection of national image towards enhancing stature and sphere of influence.
3) National Defence and security; guarantee sovereignty and independence whilst maintaining internal security.
4) Government capability to functions: Maintain order to perform and deliver minimum essential public services.
5) Public health and safety, delivering and managing optimal health care to the citizen.[55]

An infrastructure is 'critical' when the services it provides are vital to national security.[56] The list of infrastructures officially considered critical is growing in addition to the chemical sector, they are transportation, the defense industrial base, telecommunications, banking and finance, agriculture, food, water, public health, government services, emergency services, and postal and shipping.[57] Section 58 of the Cybercrimes (prohibition, prevention) Act defines Critical Infrastructure as systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country.[58] The National Cyber-security Policy of December 2014 published by the Office of the National Security Adviser (ONSA) identifies critical infrastructures to include: Communication Sector, Government facilities Sector, Manufacturing Sector, Dams Sector, Defense Sector, Chemical Sector (Oil and Gas), Power and Energy Sector, Commercial facilities Sector, Financial Services Sector, Food and Agriculture Sector, Emergency Services Sector, Transportation Systems Sector, Public Health and Healthcare Sector, Water & Waste Water systems and Information Technology Sector.[59]

On 22 November 2016, the Secretary-General informed the Security Council that control of dams had often been a strategic terrorist goal, and in the case of operations carried out by Isil,[60] Isil had used water as both a target and a weapon.[61] Isil has not only destroyed water-related infrastructure such as pipes,

---

[53] Department of Homeland Security, National Infrastructure Protection Plan (Washington, DC: Government printing office, 2009), Available at < https://www.dhs.gov/xlibrary/assets/NIPP-Plan.pdf, > accessed 2/6/2020, P.109

[54] Malaysia (2009), Available at < https://CNII,cybersecurity.org.my/main/index.httml > accessed 2/6/2020.

[55] A. Philip *etal*., 'The challenge of protecting Critical Infrastructure' Centre for Risk Management and Decision processes, Wharton University of Pennsylvania, working paper, 2005, P.5

[56] Ibid.

[57] Ibid.

[58] Section 58 of the Cybercrimes (Prohibition, Prevention) Act, 2015.

[59] National Cybersecurity Policy, December, 2014, Para. 7.5 (ii)

[60] United Nations Security Council Counter-terrorism Committee Executive Directorate, 'Physical Prosecution of Critical Infrastructure against Terrorist Attacks' CTED Trends Report, March 2017, P. 5.

[61] A Vishwanath., 'The water wars waged by Islamic State' November 2015, Available at < https://www.stratfor.com/weekly/water-wars-waged-islamicstate > accessed 2/6/2020.

sanitation plants and bridges, it has also used water as an instrument of violence by deliberately flooding towns, polluting bodies of water and ruining local economies by disrupting electricity generation and agriculture.[62]Between 2013 and 2015, Isil launched twenty (20) major attacks and countless smaller attacks against Syrian and Iraqi water infrastructure including flooding villages, threatening to flood Baghdad, closing the dam gates in Fallujah and Ramadi, cutting off water to Mosul, and allegedly poisoning water in small Syria towns.[63] Following the capture of the Ramadi dam in May 2015, Isil drastically reduced the water for the irrigation systems and treatment plants in the predominantly Shiite downstream provinces of Babil, Karbala, Najat and Qadisiya, which are among Iraq's most important agricultural centres, thereby putting the food security of the entire country at risk.[64] The production and supply of energy resources relies on a complex system of infrastructures that are among the most critical in the world. They include pipeline, rigs, refineries, flow stations, manifolds terminals, fuel cisterns, electrical energy pylons, pumps stations, processing plants, vessels and tankers.[65] Al-Qaida and its affiliates have attacked facilities and personnel of oil companies in Algeria, Iraq, Kuwait, Pakistan, Saudi Arabia and Yemen, and have also captured numerous oil fields. The UN estimates that the income generated by Isil from oil and oil products in 2015 was between $400 million and $500 millions.[66]

4. Cyber-terrorism in Nigeria: Is the threat real?

Terrorist cells in over 60 countries have resorted to the use of cyberspace to recruit their members, spread propaganda, raise money, train more terrorist and conspire to intimidate and coerce government and innocent citizens in furtherance of their political and religious objectives.[67] Social media platforms are now avenues for the terrorists' use for coordination of their illicit actions and spread of messages. Terrorists use of the internet, especially social media to propagate messages involve a mix of social media savvy, tactical use of technology, and the nature of the internet itself as an isolating yet supportive force for some people, enough to drive some to become terrorists themselves. They mostly use targeted social media campaigns by way of hash-tags to gain attention and support. The number of sites that terrorists have been using is extensive: Twitter, facebook, instagram, you tube and flickr.[68] In August 1999, it was reported that almost every terrorist group had established their individual websites, along with a mishmash of freedom fighters, crusaders, propagandists and mercenaries.[69] The internet serves as an appropriate haven for them to engage in conferences and debate on their premeditated objectives through the use of web forums, emails, and chat. The internet has the ability to connect not only members of same terrorist organizations but also members of different groups.[70]

Al Qaeda members (which are at present the most notorious terrorist group) have mastered the art of using the cyberspace to advance their own goals.[71] Osama Bin laden, Isis and Boko Haram have reportedly posted web pages on the internet to gain support and followers, and also in furtherance of the spreading of their messages.[72] The headquarters of Osama Bin Ladin in Afghanistan was reported to have been equipped with computers and communications equipment as at 1996.[73] Some Egyptian; Afghan computer experts were said to have configured a communication network that used the web, email and

---

[62] Ibid.
[63]Ibid.
[64] CTED Trends Report 2017 (n60).
[65] UNISA., African Security Review, September 2015, 'Terrorism, insurgency, kidnapping and Security in Africa's energy sector' Available at < https//www.tandfonline.com/do1/pdf/10/1080/10246029.2015.1072967 > Need access-true, accessed 5/6/2020.
[66] S/2016/92 Report of the SC on the threat posed by Isil, January 2016. Available at < https://www.un.org/en/ga/search/view.doc.asp?Symbol=S/201692, accessed 5/6/2020.
[67] C. R. Ibekwe., (n14) P. 425.
[68]Ibid.
[69] M. Ambinder., 'AlQaeda's First English Language Magazine is Here' The Atlantic, 3rd June 2010, Available at < https://www.the atlantic.com/international/archive/2010/06/al-qaedas-first-english-language-magazine-is-here/59006 > accessed 16/6/2020.
[70] M. Conway Terrorist 'use' of the internet and fighting back 2005, P. 11.
[71] J. R. Westby., Countering Terrorism with cyber-security, (2007) 47 Juris-Metris J. 297 - 313
[72] Centre for strategic & International Studies, cyberrcrime…cyber-terrorism…cyber warfare…Averting an electronic waterloo (1998), Available at < https://www.csis.org.pubs/cyberfor.html > accessed 22/6/2020.
[73] J. Arquilla *etal.,* Networks, Netwar, and Information Age Terrorism, in Countering the New Terrorism, RAND, 1999, P. 65.

electronic bulletin boards.[74]An Al Qaeda affiliated terrorist group led by Abu Musab al-zarqain, posted the second edition of its recruitment magazine as at June 2015.[75] Hamas terrorists were also reported to use chat rooms and e-mail to plan operations and coordinate activities; thereby making it difficult for Israeli security officials to trace their messages and decode the contents thereof.[76]

In Nigeria today, the greatest and predominant security challenge that the country is facing is terrorism. The jarna'atu Ahlis Sunna Ladda Watin Wal-Jihad, a religious based Islamic fundamentalist group popularly known as Boko Haram is the harbinger of terrorism in Nigeria today.[77] The sect which is predominantly based in the North Eastern part of the country has an ideology that is averse to Western education and anything it represents.[78] The sect also seeks an enthronement of Islamic (Sharia) government in the whole of Northern Nigeria. Adherents of Boko Haram attack government institutions, such as the police and military through armed attacks or suicide bombing. [79] The sect was founded by Mohammed Yusuf in 2001. Because of its claim of wanting to establish Sharia law in Nigeria, it is sometimes referred to as Yusufiya group. The unfortunate association of Islamic religion with terrorism has been as ancient as 622/623 AD when the religion was found.[80] Islam started by the sword through conquests made by Prophet Mohammed culminating in the Hijiriah from Medina to Mecca in 623 A.D.[81] The Boko Haram sects in Nigeria operates as a faceless group of militants who carryout coordinated surprise attacks on defenceless citizens by striking them at churches, markets, offices, relaxation sports etc. Usually a suicide bomber on a motorcycle, can hit its target and dies with the victims. But in June 2011, there was a significant shift in Boko Haram's targets, tactics and geographic reach. The use of a suicide VBIED on the Abuja police barrack marked the first time on record a suicide attack was carried out in Nigeria.[82] Boko Haram has international links with other terrorist groups such as the Al-Qaeda in the Magherb (AQIM), Al-Shabab in Somalia.[83] Boko Haram's evolving tactics and targeting may be the result of ties between AQIM in North Africa and Al-Shabaab in Somalia. Such cross-pollination of weapons, tactics, and bomb-making expertise had increased the capabilities of the terrorist group. On June 14, 2011, AQIM leader Abu Masab Ab al-wadoud, also known as Abdelmalik Droukdel, told Al-Jazeera that his group would provide Boko Haram with weapons, support and training.[84] In September 2011, threats made by Boko Haram to bomb Lagos Airport prompted security officials to search all vehicles approaching the airport, causing major disruptions.[85] Even more indicative of the growing sophistication and threat potential of Boko Haram is the groups increased use of the internet forums. According to a September 28, 2011 report published by the SITE intelligence group, Boko Haram had developed an increased online presence that seems to have contributed to the rapid increase in their strength.[86]The sect has been getting tremendous support from these groups. It is becoming increasingly

---

[74] Ibid.

[75] See Abu Musab al-zargawi internet magazine showing its second recruitment. Available at < https://www.adl.org/main-terrorism/qaedamag-2-62005 html > accessed 22/6/2020.

[76]J. Arquilla *etal.*, (n73), P. 1

[77] Text of the speech delivered by Col.Sambo Dasuki at the third seminar held at the National Defence College, Abuja by the Alumni of the Institution Published on the 1st day of February 2013 in leadership newspaper.

[78] J.A.M Agbonika and J.A.A. Agbonika., The Nigeria Security Challenges: Boko Haram and Human Rights Perspective, Rivers State University of Science and Technology Journal of Public Law Vol. 2013, P. 173.

[79]K. Joseph., West Africa and Islam: What every Catholic should know, (Ibadan Nativity Press, 2004), PP. 20-25

[80] T. Barga., Terrorism and violence as a challenge to Christian Evangelization in Nigeria, Vol. 20 June 2012, Jos studies; published by St. Augustine Seminary.

[81] Ibid.

[82] Sub -committee on counterterrorism and intelligence. Committee on Homeland Security, House of Representatives 'Boko Haram Emerging threat to the US. Homeland, First Session, December 2011.

[83] Ibid.

[84] S. Stewart., 'The Rising Threat from Nigeria's Boko Haram Militant Group' Strafor Global Intelligence, November 10, 2011, Available at < https://www.strafor.com/weekly/20111109-rising-threat-nigeria's boko haram.militant-group > accessed 4/6/2020.

[85] E. Chidiogo., 'Bomb scare disrupts Lagos Airport road activities, Daily Times NG September 24, 2011.

[86] B. Roggio., suicide bomber hits UN office in Nigeria Capital, the long War Journal, August 26, 2011.

clear that as technology advances, the tools used by the sects in their destructive and terrorist activities will no longer be guns, and bombs but other weapons of mass destruction and attacks on critical infrastructure using the computer.

5. The Cybercrimes (Prohibition, Prevention) Act 2015

In the wake of advancement of technology, several conventional crimes which were hitherto only committed against per sons physically or in direct contact with the assailant or criminal has now shifted to the internet where such offences can be committed over the internet with the use of the computers and without the victim even getting to know or meet the offender.[87] This ugly development amongst other factors necessitated the enactment of the cybercrimes Act[88]in Nigeria.[89]

The cybercrime Act was Signed into law on May 15, 2015.[90] The Act provides an effective, unified and comprehensive, legal, regulatory and institutional framework for the prohibitions, prevention, selection, prosecution and punishment of cybercrimes in Nigeria. The Act is made up of 59 sections, 8 parts and 2 schedules. The first schedule which is section 42(1) lists the members of the cybercrime Advisory council. The second schedule which is section 44(2) (a) provide for businesses to be levied for the purpose of the cybersecurity fund.[91]

The Act covers broad spectrum of list of cybercrime offences punishable with penalties and fines in part III., which includes offences against critical national information infrastructure, unlawful access to computers, system interference, interception of electronic messages, e-mails, electronic money transfer, Tampering with critical infrastructure, wilful misdirection of electronic messages, unlawful interception, computer related forgery, computer related fraud, theft of electronic devices, unauthorized modification of computer systems, network data and system interference, cyber-terrorism, fraudulent issuance of e-instructions, identify theft and impersonation, child pornography and related offences, cyberstalking, cybersquatting, Racists and xenophobic offences, importation and fabrication of e-tools, breach of confidence by service providers, manipulations of ATM/POS terminals, phising, spamming, spreading of computer virus, dealing in card of another, purchase or sale of card of another, use of fraudulent device or attached e-mails and websites.[92]

Part II of the Act specifically provides for the protection of Critical National Information Infrastructure[93] while section 18(1) of Part III provides for the offence of cyber-terrorism. The section provides as follows:

> A person who accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable to life imprisonment.[94]

The Act seems elaborate but it may not be able to effectively address the issue of cyber-terrorism and the protection of critical national information infrastructure owing to several pitfalls in the Act. First, the law do not provide for a single enforcement institution. Section 41 (1) vest the enforcement of the Act on the National Security Adviser while section 41(2) and section 52(1) and (3) vest the powers of enforcement of the Act on the Attorney-General of the Federation. This is capable of creating conflict in the enforcement of the Act. Secondly, Nigeria over the years is fond of appointing retired military personnel as National Security Adviser. Sadly enough, most of these retired military officers so appointed are actually novice in cyber security which is quite different from conventional security. The Act did not spelt out what should be the qualification of the National Security Adviser. Moreover, the duties assigned to the office of the National Security Adviser by virtue of section 41(1) of the Act are too technical to be left

[87] N. Itanyi., 'Technology and Hate speeches in Nigeria: Is the Nigerian Cybercrimes Act 2015 Adequate in Felix E. Eboibi (ed), Handbook on Nigerian Cybercrime Law, (Justice Jeco Printing and Publishing Global, 2018), P.333
[88] Cybercrimes (Prohibition, Prevention) Act. 2015
[89] N. Itanyi., (n87) P. 333
[90] Cybercrimes Act 2015
[91] Section 42(1) and 42(2) of the Act.
[92] See Part III of the Cybercrimes Act 2015
[93] Part II of the Act.
[94] Section 18(1) of the Act.

in the hands of a National Security Adviser who may not have any knowledge of Cyber-Security. The duties require someone with adequate knowledge of cyber and computer related issues.

6. Practical Challenges to Prosecuting Perpetrators of Cyber-terrorism.

The Prosecution of Perpetrators of Cyber-terrorism is not without challenges. Some of the identified challenges affecting the effective prosecution of cyber-terrorism offenders are: Jurisdictional issues, Evidential issues and Extradition. These factors militating against the effective prosecution of perpetrators of cyber-terrorism are treated below:

a) Jurisdictional Issues

While the world we live in is physically demarcated in boundaries and territories, the world of cyberspace does not recognize any physical or political barriers or national frontiers.[95] In plain words, cyber world is transnational, a global medium devoid of any territorial divisions.[96] The unbounded nature of the internet has challenged the basis for the traditional notions of jurisdiction which are predicated on real space demarcation.[97] Because, a page on a worldwide web can reach web surfers in every state in the nation and perhaps every nation of the earth, there arises the issue of where exactly a person who has a cause of action, based upon web transaction may sue.[98]

In order for any court of law to try and punish a cyber-terrorist, such a court must be cloth with the legal authority to do so. The legal authority that empowers a court to so Act is referred to as jurisdiction. In simple words, jurisdiction is the power of a court to hear and determine a case.[99] Jurisdiction is the legal capacity of a court to hear and determine judicial proceedings. It is the power to adjudicate concerning the subject matter of the controversy.[100] A court of Law can only exercise judicial powers when it has jurisdiction.[101] Without jurisdiction, a court's judgement will be ineffective and impotent.

The determination of Jurisdiction in respect of cyber-terrorism offences could be cumbersome and mostly difficult for the courts to determine.[102] The virtual world seems to be a borderless Journey to the wonderland.[103] This has continued to cause confusion and misapplication of legal principles for the enforcement of cyber-terrorism adjectival laws.[104] For instance, in the case of ***R. v. Governor of Brixton Prison and Anor, Ex-parte*** Levin,[105] Where one of the issues for determination was whether the *locus in quo* of the offence was in St. Petersburg, Russia, where the computer instructions were sent, or in victim's computers in Parsippany, New Jersey in United States. The Court held that given the virtually instantaneous nature of electronic transaction, it was 'artificial' to regard the offence as having occurred in one place or the other.[106] Could it then have been right to say that cyber-terrorism offences lack any *locus delicti;* or could the offences be said to have multiple *locus delicti*? Since cyber-terrorism offences are usually cross-border offences involving multiple Jurisdictions; which state could rightly assume Jurisdiction? These Questions have necessitated the need for various states to include provisions conferring the national courts with extra territorial jurisdiction.[107]

b) Evidential issues

Criminal Prosecutions can succeed or fail based upon the evidence presented. Loss or contamination of evidence in the cause of cyber-terrorism investigation is a very common and also an obvious problem

---

[95] K. Seth., (n 1) P. 31
[96] Ibid.
[97] Ibid. P. 32
[98] Ibid.
[99] Ibid.
[100] *Otukpo v. John* (2000) 8 NWLR (Pt. 669) 507 at 526
[102] *Bronik Motors Ltd v. Wema Bank Ltd* (1983) 6 SC 158
[103] A. M. Weber., 'Council of Europe's Convention on Cybercrime' (2003) Berkeley Tech LJ, 18, 425.
[104] S. W. Brenner., 'Cybercrime Jurisdiction' (2006) 46 (4-5) crime, law and social change.
[103] C. R. Ibekwe., in F. E. Eboibi (ed), Handbook on Nigerian Cybercrime Law, (n14) P. 443
[105] (1997) Q. P. 65
[106] *Supra*, at P. 81 Per Beldam LJ.
[107] M. Hilderbrandt., 'Extra territorial Jurisdiction to enforce in, cyberspace' (2013), University of Toronto Law Journal, 63 (2), 196-224.

which may affect the veracity to be attached to the piece of evidence, or even jeopardize the entire Criminal Proceedings.[108] The collection of data outside the physical, territorial boundaries have also proven to be one of the most important issues that could also paralyse cyber-terrorism investigations and any consequential prosecutions.[109] Prosecutors of cyber-terrorist will often have problems getting access to relevant documents. Where documents are available, the courts will face special challenges in verifying whether they are authentic. Also, obtaining witness testimony is quite difficult. The process of compelling witnesses who can give direct testimony is quite cumbersome sometimes owing to the distance involved.

c) Extradition

The prosecution of cyber-terrorists sometimes involves one state requesting the extradition of a suspect from another state. Extradition laws generally provides for a complex legal process which can take months if not years to reach its conclusion. Also, many states usually refuse the extradition of their own nationals who have taken refuge in their territory, although as between states who observe absolute reciprocity of treatment in this regard, request for surrender are sometimes acceded to.[110] International Law concedes that the grant of and procedure as to extradition are most properly left to municipal law, and does not, for instance, preclude states from legislating so as to refuse the surrender by them of fugitives, if it appears that the request for extradition had been made in order to prosecute the fugitive on account of race, religion, or political opinions or if the fugitive may be prejudiced thereby upon eventual trial by the courts of the requesting state.[111]

CONCLUSION

The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature.[112] In the age of information technology, the terrorist have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produce would be almost irreversible and most catastrophic in nature.[113] Cyber-terrorism, being a global menace, it is impossible to combat it without international harmonization of laws on the subject and a concerted effort by the international society.[114] As terrorism is being fought through regional and International Cooperation, so also cyber-terrorism can be thwarted only when nations come together and make positive move.[115]

Nigeria as a country has enacted the cybercrimes (Prohibition, Prevention) Act 2015, but the Act alone cannot fortify the country against cyber-terrorism attack owing to the transnational nature of the cyberspace. Nigeria needs to join the International Community to combat cyber-terrorism in order to effectively combat the menace at home. Nigeria has not yet signed nor ratified and accede to the convention on cybercrime. The convention on cybercrime adopted by the council of Europe on 8 November 2001, is the first international treaty on crimes committed via the internet and other computer networks.[116]The main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[117] Cooperation at this level is of course the most powerful way of ensuring a consistent

---

[108]E. Murphy., 'The new forensics: Criminal Justice, false certainty, and the second generation of scientific evidence' (2007) California Law Review 721-797.

[109] A. Singh Poonia., A. Bhardwaj and G.S Danyaryach., 'Cybercrime: Practices and Policies for its prevention: (2011), In the First International Conference on Interdisciplinary Research and Development, special No. of the International Journal of the Computer, the Internet and Management (Vol. 19), Available at <https:inrit-2015.com/inrit 2011/proceedings 2011/02-49-23A – Aject % 20 poonia-%5B9 % 5D. pdf. > accessed 5/6/2020.

[110] I. A. Ashearer., Starkes International Law, (London, Butterwortts, Eleventh (ed) 1994), P. 318

[111] Ibid.

[112]R. K. Chanbey., (n5), P. 497

[113] Ibid.

[114]T. Fatima., Cybercrimes, (Eastern Book Company, India, 2011) P. 214

[115] Ibid.

[116] D. R. Johnson & D.G., post, 'Law and Borders: The Rise of Law in Cyberspace' Available at < https://www.eli.org/x0025LBEIN.html > accessed 6/6/2020.

[117] T. Fatima., (n114), P. 125

international approach to the problem of cybercrime ultimately helping in eradicating cyber-terrorism too.[118] A global security agenda (GSA) was launched by the International Telecommunication Union in Geneva in May 2007. The GSA strives to provide a global framework for dialogue and international co-operation. Its objective is to coordinate an international response to the increased challenge to cybersecurity and to enhance confidence and security in the information society.[119] The GSA also calls for the development of cybercrime legislation that is globally applicable and consistent with existing national and regional legislative measures.[120]

In order to effectively combat the menace of cyber-terrorism in Nigeria and protect critical information infrastructure, this paper makes the following: recommendations.

1. The amendment of the cyber-crime (Prohibition Prevention) Act 2015, to include the creation of a specialized Cyber Attack Prevention Agency.
2. The Nigerian Government should immediately sign and ratify the cybercrime convention adopted by the council of Europe which came into force on 1st July, 2004.
3. Nigeria should become involved in the Global Security Agenda of the International Telecommunication Union (ITU), as such an initiative will enhance its cybersecurity measures.

[118] Ibid.
[119] M. Gerke., 'Understanding Cybercrime' 2009, Available at < https://www.itu.int/ITU-D/cyb/cyberseurity/legislation/html. > Accessed 4/6/2020.
[120] Ibid.