Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.33, 2015
www.iiste.org

Cyberterrorism: A Comparative Legal Perspective

Mu'azu Abdullahi Saulawa[1*] Junaidu Bello Marshal [2]
1. Faculty of Law, Umaru Musa Yar'adua University, P.M.B. 2218. Katsina State, Nigeria
2. Faculty of Law, Usmanu Danfodiyo University, P. M. B 2486. Sokoto State, Nigeria
* Email- muazu.abdullahis@gmail.com

Abstract
The paper focuses on cyberterrorism and a comparative legal perspective with a view to examine the cyberterrorism as a concept as well as its definition. The revolution of development of Information and Communication Technology (ICT) has changed society to be a point where advances in programming computer and intelligence software operates in a higher processing capacity. The uses of desktop or laptops computers are leading the society to a time where or when cyber used to perpetrate various act of offences. The paper analyses legal perspective that introduced the Cybercrime Convention in Europe in relation to cyber terrorism and the opening to other Member States, while Economic Community for West African States (ECOWAS) issues a Directive to Member States to adopt enabling laws so as to combat the practices of cybercrime in relation to cyber terrorism. The paper argues that Nigerian Cybercrime Act 2013 is an established law that addresses the endemic practice of cybercrime and provides for cyber terrorism. Further, the paper examines the Nigerian financial regulators like the Central Bank of Nigeria (CBN), the Economic Financial Crimes Commission (EFCC) and other Units mandated to curb the money laundering and combating the financing terrorism and other financial institutions related crimes. The paper relies on primary and secondary sources of data and the analysis is descriptive in nature. The paper will proffer recommendations and conclusions for effective measures for proper implementation and enforcement.
Keywords: Cyberterrorism, definition of cyberterrorism, Relevance of cyberterrorism in cyberspace, Comparative Legal Perspective

1. Introduction

The paper focuses on cyberterrorism and a comparative legal perspective. The number of threats posed by cyberterrorism has completely and overwhelmingly attracts global attention. The security of environment and the ICT industry are not safe, the variety use of sophisticated cyber terrorist electronically equipment's hacking into computers that control dams, air traffic control system, endangering the lives of millions and the nation's security. Yet despite all predictions of cyber-global acceptance no single example of real cyber terrorism has been recorded. [1]

The cyberterrorism threat is real, with the constant used of infrastructures and most of such in western countries is networked through computers; the potential cyberterrorism is, to be sure very alarming. Nothing can be further from the truth, hackers, although not motivated by the same objective that inspires terrorist that have demonstrated individuals can gain access to sensitive information and to execute an operation which is crucial. Terrorists, at least in theory could thus follow the hackers' lead and broke into government or private computers cripple, damage or at least disable financial sector, military and economies. [2]

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

2 Definition of Cyberterrorism

In defining cyberterrorism, a number of contributions have been used, according to Federal Bureau of Intelligence (FBI):

> …terrorism includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. [4]

Cyberterrorism is further defined as the:

> the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by

[1] Gabriel Woimann, ''Cyberterrorism How Real is the Threat? , United States Institute of Peace, Special Report 119, December 2004, at p. 2.
[2] Ibid.
[3] Ibid.
[4] Code of Federal Regulations, 28 C.F.R.Section 0.85 (July 2001): 51.

subnational groups or clandestine agents. [1]

However, in an attempt to have a recap and comprehensive definition of cyberterrorism, one and most notably definition by Dorothy Denning, a professor of computer science and security expert has admirably comes forward with a definition that

"... politically motivated hacking operations intended to cause
grave harm such as loss of life or severe economic damage."[2]

Cyberterrorism can be traced back to the early 1990s, when the rapid growth of internet use and the debate on the emerging 'information society' sparked several research and studies on the potential risks faced by the highly networked high-tech dependent by the United States. As only in 1990, the National Academy of Sciences began a report on computer security with the words 'we are at risk'. Increasingly, American depends on computers…. Terrorism has the opportunity of doing more damage with a computer key board than with a bomb. [3]

The September 11, 2001 (9/11) of terrorist attacks that the world appears to be at the peak of the boarders in which countries are vulnerable to invasion through information, ideas, people and materials in short an open world with no defence.[4]

After the 9/11 attack, security and terrorism has become a tropical discourse due to the prominent attack. Although the attacks tend to be psychological, religious, political and economic forces surrounding and thus have combined to promote the fear of cyberterrorism. [5]

3. Relevance of Cyberterrorism in Cyberspace

Cyberterrorism is a transformed strategy and an attractive alternative to terrorist in perpetrating their acts, particularly in the current trend. Terrorist preferred to use of cyberspace as a new trend in achieving their targets than the customary aspects. As it proves to be cheaper, easier than the traditional terrorist methods and what the terrorist needs is a personal computer and on online connection. That further conceal the terrorist identity and not need to buy weapons, guns and explosives instead they create and deliver computer virus through wireless connection, cable and telephone lines. [6]

Usually, the targets are enormous. It is the working of cyberterrorist to targets computer and government related networks, individuals, private corporations' for instance private airlines, public café and etc. The continued acts of cyber terrorist identify number and complexity potential targets in believing that it is easy for terrorists to exploits weakness and vulnerabilities.[7]

Cyberterrorist usually targets critical infrastructures such as electric power grids and emergency services are vulnerable to a cyber-attacks because the infrastructures and the computer systems are run at highly complex making it an effective and impossible to do away with any difficulty.[8]

The advantages exploits by terrorism is anonymity because cyber terrorism can be remotely used in achieving targets, the act requires less physical appearance or training or other disclosure forms of cyberterrorism, but making it easier for terrorism organizations in recruit and retain of followers. [9] The other concerned part of cyberterrorism is the potential targets to affect directly a large number of people than the old-fashioned terrorist methods, thereby generating media attention which is the final score of terrorist goal.

In this era of cyberterrorism, critical areas such as financial institutions of any nation are vulnerable to financial terrorism from internal and external sources. In this regard, it is important to consider this as vital component of national security. This means that banks and other financial institutions must be exposed to both physical security and soft security orientations in their daily operations.

It is also important to state that with the current discontent on the global economic order, virtual criminals have become more tempting to vent their anger on reputable corporations, national government and financial institutions. Therefore, all over the world, there is mounting concern on the dangers of financial

---

[1] Pollitt, Mark M. "CYBERTERRORISM - Fact or Fancy." Georgetown University. Department of Computer Science. 10 June 2009, available at www.cs.georgetown.edu/~denning/infosec/pollitt.html.

[2] Dorothy Denning, "Activism, Hactivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, eds., Networks and Netwars, (Rand 2001), p. 241. Dorothy Denning, Is Cyber War Next? Social Science Research Council, November 2001, at http://www.ssrc.org/sept11/essays/denning.htm].

[3] Ibid.

[4] Gabi et tal, 'The Threat of Terrorist Organizations in Cyberspace', Military and Strategic Affairs, Vol. 5, No. 3, December 2013.

[5] Gabriel Woimann, op. cit at p. 3.

[6] Ibid. at p. 6.

[7] Ibid.

[8] Ibid.

[9] Ibid.

terrorism perpetuated through the ICT enabled virtual world. The state of affairs now is that nations and other stakeholders can ignore early warning signs of cyberterrorism at their own peril[1].

4. Comparative Legal Perspective

The comparative legal perspective covers the discussion on the provisions of the Act and Regulations which includes the Council of Europe Convention on Cybercrime, ECOWAS Directive on Fighting Cybercrime and Cybercrime Act 2013. The comparative perspective further examines the Regulation of CBN on Money Laundering and Combating the Financing Terrorism, EFCC in relation to existing Unit that has mandate in addressing money laundering and financing terrorism.

4.1 Council of Europe Convention on Cybercrime

The Convention on Cybercrime opened for signature in Budapest, November 23, 2001 and entered into force in 2004.[2] It aimed to meet this challenge respecting human rights is the new reality now called the information societies.

Article 22 provides that Member countries must enact law enabling them to have jurisdiction over all the previous crimes described in the convention should they occur in any one of the four places: [3]

a. In its territory; or
b. On board a ship flying in the flag of that party; or
c. On board an aircraft registered under the laws of that party; or
d. Outside the territory of the country but committed by one of its nationals.

A party would establish territorial jurisdiction of the person attacking the computer system and the victim were located within the country, or where the victim was inside the territory and the attacker was not.[4]

The jurisdictional theory in the Article is determined by the place where the offence of cyberterrorism is committed in whole or in part.[5] The Convention relies exclusively on the territoriality or nationality theories to empower parties to establish jurisdiction. [6]

4.2 ECOWAS Directive on Fighting Cybercrime

The objective of the Directive is to adopt the substantive criminal law and the criminal procedure of ECOWAS Member States to address the cybercrime phenomenon. [7]

The scope of the Directive shall be applicable to all cyber-related offences within ECOWAS sub-region as well as to all criminal offence whose detection shall require electronic evidence. [8] The Articles in the Directive further discussed related offences in user of information and communication technology.[9]

The Article provides that the use of information and communication technology to commit common law offences such as theft, fraud, possession of stolen goods, breach of trust, extortion, terrorism and money laundering or organized crimes shall constitute a higher degree of offence than common law offences.[10] The main concerned of the Article is the cyberterrorism, although the Directive did not fully provides for a provision which solely discussed cyberterrorism but the fact is that the use of ICTs in a related offence of terrorism constitute cyberterrorism which is punishable under the law.

The Article further provides that theft, fraud, possession of stolen goods, breach of trust, extortion, act of terrorism and counterfeiting relating to computer data, software and programme shall constitute an offence. [11]

---

[1] Hugo Odiagor, 'Cyber terrorism and Nigeria's Economy' (2011) available at www.vanguardngr/2011/11/cyber-terrorism-and-%E2%80%99s-economy/> Accessed on 12/12/2014.

[2] According to Article 36 provides for the 'Signature and Entry into Force' allows non-Council of Europe States to become signatories. In addition to COE of States who had participated in the drafting of the Convention. For a list of the States that signed and ratified the Convention, see 'Convention on Cybercrimes CETS No.: 185, online at http://convention.coe.int.

[3] Ibid, Council of Europe Convention on Cybercrimes

[4] Explanatory report of the comm. Of ministers of the convention on cybercrime 109th session (adopted on November 8, 2001)

[5] Armondo Cottim, 'Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime. European Journal of Legal Studies, vol… Issue 6, at p. 2, available at htpp://www.ejls.eu/6/78UK.htm. Accessed on 14/11/2014.

[6] Ibid. at p. 4.

[7] The full meaning of ECOWAS is Economic Community of West African Countries. Article 2 of the Directive C/DIR. 1/08/11 on Fighting Cybercrimes Within ECOWAS, Sixty-Sixth Ordinary Session of the Council of Ministers.

[8] Article 3, Ibid.

[9] Chapter II, Ibid.

[10] Article 24, Aggravating Circumstances of Common Law Offences, Ibid.

[11] Article 25, Violations of computer Data, Software and Programme, Ibid.

4.3 Nigeria Cybercrime Act 2013

The objectives of this Act are to -[1]

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
(b) ensure the protection of critical national information infrastructure; and
(c) promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

The application of this Act shall apply throughout the Federal Republic of Nigeria[2]

The Act provides for Cyberterrorism [3] and also provides that Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and liable on conviction to life imprisonment. [4] The Act further provides for the purposes of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended. [5]

The Nigerian legislation on Cybercrimes Act 2013 clearly provides for cyberterrorism and the Act is an offshoot of Council of Europe Convention Cybercrime and ECOWAS Directive on Fighting Cybercrime. The realization of this Act by the Nigerian Government has addressed the complexity in Article 22 of Council of Europe on issue of nationality, territoriality and jurisdiction. The offences in the Convention, ECOWAS Directive all encompassed an established criminal law model for all the nations.

4.4 Central Bank of Nigeria Regulation on Financing Terrorism

CBN has its own regulations in fighting terrorism in the nation with an aim of coordinating fund that may be used in cyberterrorism. The Federal Government of Nigeria has enacted CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations 2013 (AML/CFT).

The objectives of the regulations as provided in part I of the Act are[6]:

To AML/CFT compliance guidelines for financial institutions under the regulatory purview of CBN as required by the relevant provision of the Money Laundering (Prohibition) Act, 2011 (as amended), the Terrorism Prevention Act 2011 (as amended) and other relevant laws and regulations.[7] To enable the CBN to diligently enforce AML/CFT measures and ensure effective compliance by the financial institutions and [8] provides guidance on Know Your Customer (KYC) measures to assist financial institutions in the implementation of these regulations. [9]

The scope of these Act cover the relevant provision of Money Laundering (Prohibition) Act 2011 (as amended), the Terrorism Prevention Act 2011 (as amended) and other relevant laws and regulations. [10]

The Act provides for Anti-Money Laundering and Combating the Financing Terrorism Directives.[11]

The Act provides that a financial institution shall adopt policies stating its commitment to comply with Anti-Money Laundering (AML) and Combating the Financing Terrorism (CFT) obligations under subsisting laws, regulations and regulatory directives and to actively prevent any transaction that otherwise facilitates criminal activities, money laundering or terrorism.[12]

The Act also provides that a financial institution shall formulate and implement internal controls and other procedure to deter criminals from using its facilities for money laundering and terrorist financing.[13] And financial institutions shall adopt a risk-based approach in the identification and management of their AML/CFT risks in line with the requirements of these Regulations.[14] The financial institutions shall comply with request made pursuant to current AML/CFT legislations and provide information to the CBN, Nigeria Financial Intelligence Unit (NFIU) and other competent authorities.[15]

The Act further provides that financial institutions shall not in any way inhibit the implementation of

---

1 Section 1, Cybercrime Act 2013.
2 Section 2, Ibid.
3 Section 17, Ibid.
4 Section 17 (1), Ibid.
5 Section 17 (2), Ibid
6 Section 1, Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations 2013.
7 Section 1 (a) Ibid.
8 Section 1 (b), Ibid.
9 Section 1 (c), Ibid.
10 Section 2 (1), Ibid.
11 Part II of the Act and also Anti-Money laundering and combating the Financing Terrorism means (AML/CFT), Ibid.
12 Section 4 (1), Ibid.
13 Section 4 (2) Ibid.
14 Section 4 (3) Ibid.
15 Section 4 (4) Ibid.

the provisions of these Regulations and shall co-operate with the regulators and law enforcement agencies in the implementation of a robust AML/CFT regime in Nigeria. [1] It also provides that financial institutions shall render statutory reports to appropriate authorities as required by law and shall guard against any act that will cause a customer or client to avoid compliance with AML/CFT Legislations.[2] That financial institution shall identify, review and record other areas of potential money laundering and terrorist financing risks not covered by these Regulations and report same to the appropriate authorities.[3]

The Act further provides that financial institutions shall reflect AML/CFT policies and procedure in strategic policies.[4] That financial institution shall conduct on-going Due Diligence on all business relationships and shall obtain information on the purpose and intended nature of the business relationship of their potential customers.[5] And finally, the financial institutions shall ensure that their employees, agents and others doing business with them, clearly understand the AML/CFT programme.[6]

The relevance of the regulations to the cyberterrorism is in connection to transfer of funds and usually sponsored by a different institutions/organizations where it involves terrorism and that has to go through the financial institutions across the country in monitoring the activities of terrorism by the financial intelligence unit.

4.5 Economic and Financial Crime Commission Act on Financing Terrorism

The Economic and Financial Crime Commission [7] was established in 2004 by the Federal Government of Nigeria and its aim is to combat economic and financial crimes. The objectives of the EFCC have now widened to create a Unit that cover Anti-money laundering, financing terrorism and other financial institutions in Nigeria. The Special Control Unit against Money Laundering (SCUML) was established as a Special Unit of the Federal Ministry of Commerce and Industry by the Federal Executive Council of Nigeria in September 2005.[8] The SCUML mandate is to 'monitor, supervise and regulate the activities of all Designated Non Financial Institutions (DNFIs) in Nigeria in consonance with the country's AML/CFT regime.[9]

The SCUML also collaborates with the office of Economic and EFCC in efforts to serve as a structure for curbing Money laundering and Terrorist Financing in the DNFI sector and sanitizing the sector to create a qualify a window opportunity for promotion of commerce and investment, it ensure effective supervision of DNFIs which includes amongst other, registration, inspections on a risk based-approach, ensuring a rendition of statutory reports (cash-based transaction reports, currency transaction reports, suspicion transaction reports), training and manpower development.[10]

The NFIU, an operative Unit in the office of EFCC and was established under EFCC (Establishment) Act 2004 and Money Laundering (Prohibition) Act of 2004, amended (2011).[11]

The NFIU coordinating objective is receipt and analysis of financial disclosure of Currency Transaction Report and Suspicion Transaction Report in line with AML/CFT regime, NFIU also circulate intelligence gathered thus to competent authorities. The NFIU also draws its responsibilities directly from the 40+9 Special Recommendations of the Financial Action Task Force (FATF), the global coordinating body for AML/CFT. The law requires financial institutions and designated non financial institutions to submit records of financial transactions to NFIU. [12]

Flowing from the above legal comparative perspective of the entire analyzed Act and the regulations, they relate to CBN in fighting money laundering and financing terrorism across the nation. The analysis proved that money laundering is a classify forum of terrorist using charitable organizations/institutions in sourcing funds for terrorism. The role played by the financial institutions in financing terrorism is huge and these financial institutions stand as a medium in wire transfer, buying devices and coordinating terrorist fund. Some organizations are shadows, they operate outside their scope and any terrorist attacks conducted within the cyberspace become cyberterrorism. The CBN, EFCC, SCUML and NFIU collaborate all in efforts to combat the

---

1 Section 4 (5) Ibid.
2 Section 4 (6) Ibid
3 Section 4 (7) Ibid.
4 Section 4 (8) Ibid.
5 Section 4 (9) Ibid.
6 Section 4 (10) Ibid.
7 The Economic and Financial Crime Commission was popularly known as EFCC and such will be used in the paper.
8 'Special Control Unit Against Money Laundering', referred as SCUML, a report prepared by Security, Justice and growth. Online available at www.j4a-nigeria/joomdocs/Special_Control_Unit_Against. Pdf. Accessed on 20/11/2014.
9 Ibid.
10 Economic and Financial Crime Commission (EFCC)- Special Control Unit Against Money Laundering (SCUML). Available at http://efccnigeria.org/efcc/index.php/scuml. Accessed on 20/11/2014.
11 Economic and Financial Crime Commission (EFFC)- Nigeria Financial Intelligence Unit (NFIU). Available at http://efccnigeria.org/efcc/index.php/nfiu. Accessed on 20/11/2014.
12 Ibid.

practices of AML/CFT in Nigeria. This highlights the importance of their Regulations/Act in relation to cyber terrorism.

5. Conclusion

The developments of internet grow rapidly, at the initial stages was unregulated with the open architecture of cyberspace where it becomes a public domain. Cyberterrorism gives a window opportunity to the terrorist to focus their targets through cyberspace from anywhere in the world, at a cheaper cost with a high level of privacy and in an open place with ample time. The Convention on Cybercrime was designed to help realize the objective of reducing or combating the menace of cybercrime and it shows itself to be lacking particularly in the definition of cyberterrorism.

Therefore, we recommend that a further efforts need to be formalize to countries with the legal and regulatory implication arising from the use of ICT and e-commerce. The ECOWAS Directive is a piece of guide to Member States in adopting or enacting legislation covering cyberspace, cybercrime and cyberterrorism though it is an open and close Directive. The Cybercrime Act 2013 enacted by the Nigerian Government so as to capture the nomenclature of cybercrime, it accordingly succeeded. Therefore, the government shall in conjunction with other stakeholders create a Unit of cyber-security experts. The paper analysed the Nigeria laws meant to regulate the financial transactions in the form of Money laundering and combating the financing terrorism and other financial institutions crimes in Nigeria. The factor that could steer the success of this Act and Regulations is the full compliance for proper implementation and enforcement and to consider not shielding the objective of the Act.

References

Central Bank of Nigeria (2013) (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations.

Council of Europe Convention on Cybercrime 2001.

Cybercrime Act 2013.

Dorothy Denning, (2001), Is Cyber War Next? Social Science Research Council.

Gabi Siboni, Daniel Cohen, Aviv Rotbart, (2013), 'The Threat of Terrorist Organizations in Cyberspace', Military and Strategic Affairs, Volume 5, No. 3.

Gabriel Woimann, (2004), ''Cyberterrorism How Real is the Threat? , United States Institute of Peace, Special Report 119.

Pollitt, Mark M. (2009), "CYBERTERRORISM - Fact or Fancy." Georgetown University. Department of Computer Science.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar