National Journal of Cyber Security Law
Volume 1, Issue 1
www.stmjournals.com

Cyber-Terrorism: Legal and Policy Options for Coordinated National Preparedness

Isa Ali Ibrahim Pantami[1], Femi Daniel Esq.[2,*]
[1]Director General- National Information Technology Development Agency
[2]Technology Lawyer; Author- COMPUTER LAW IN NIGERIA (2015)

Abstract

Improved youth literacy juxtaposed with high unemployment rate plus fundamental historical and religious distrust makes a perfect recipe for cyber-terrorism to thrive. Cyber-terrorism has become the newest and biggest potential expression of terrorism globally. While 9/11 opened a new vista in international terrorism, the Stuxnet cyber-attack on Iranian nuclear facility (2010), Wannacry virus attack (2017) et al. demonstrates the latent capacity of the cyber-terrorist in achieving his devious purpose using technology. This paper explains some fundamentals of cyber-terrorism, its potential damaging effect on critical infrastructure and its possible deployment as an instrument of mass disruption and destruction. It also canvasses policy options to be considered to reduce the effect of an attack. Scholarly articles and commissioned papers were reviewed on the subject. This paper however, uniquely discusses the subject from a Nigerian cyber security policy, strategy and law perspective.

Keywords: *Cyber-terrorism, Cyber security, Stuxnet, Wannacry*

****Author for Correspondence*** E-mail: femigdaniel@gmail.com

INTRODUCTION

The term cyber means anything relating to computers or computer network [1]. Therefore, cyber includes but not limited to computers- software, hardware and middleware; internet, telecommunication satellite etc. Reference to 'cyber' in this paper would relate mostly to the internet with clarifications made where necessary.

The internet has become the largest and most effective communication tool invented by man. The rate of global access to the information superhighway in recent times is phenomenal. Nigeria which used to be a laggard in the internet evolution and revolution has caught the bug. Nigeria is now a global leader in internet access population. The reason for this could be ascribed largely to the successful introduction of the global satellite mobile communication network (GSM). This was done after a world-acclaimed transparent bidding and licensing rounds. This singular success has a lot of multiplier effect in terms of capital inflow, technology transfer, opening up of Nigeria to the global technology market, popularisation of smartphones and increasing demand for internet access.

Nigeria, however, has been a country on the tethers right from its cradle of independence. The multi-ethnic, multi-religious setting has created room for mutual suspicion, envy, egotism, injustice, brigandage and a bloody civil war. A nation such as this is no stranger to internally and externally propelled terrorism. The vicious circle of deaths has been oft repeated simply because there is no sustained and genuine socio-political will to deal effectively with the malaise. Another underlying factor is the lack of aggregated academic thought on the problems of terrorism in Nigeria. This paper therefore, sets out to examine the problems of defining terrorism, the precipitators of terrorist activities and implications of terrorism on critical national information infrastructure. It further reviews a major cyber-terrorist attack on the Iranian Industrial complex. The country's legal framework for tackling cyber-terrorism was analysed with the author's suggested mitigation measures to curb Nigeria's cyberspace vulnerabilities.

Virtually every terrestrial phenomenon now has its 'cyber' expression. Like terrorism, cyber law is also generating a lot of attention.

Jay Dratler Jr., dismissed the hype about cyberlaw when he posited, *much of the hoopla about 'cyberspace law' relates more to climbing the steep learning curve of [the Internet's] technological complexities than to changes in fundamental legal principles* [2]. Cyber terrorism could also be looked at from this perspective. In this new vista, scholars are discovering how to grapple with what the terrorists have understood long ago. Cyberspace only offers a new technique for advancing their age-long philosophies of violence, hatred and division.

DEFINING TERRORISM

A lot of intellectual and material efforts have been expended by government and other stakeholders to have a comprehensive definition to terrorism, all to no avail.

An erudite author put the issue grimly when he wrote- *"Above the gates of hell is the warning that all that enter should abandon hope. Less dire but to the same effect is the warning given to those who try to define terrorism* [3]*".*

Alex P. Schmid made one of the earliest attempts to define terrorism in 1983 he said:
Terrorism is a method of combat in which random or symbolic victims serve as an instrumental target of violence. These instrumental victims share group or class characteristics that form the basis for their selection for victimization. Through the previous use of violence or the credible threat of violence, other members of that group or class are put in a state of chronic fear (terror). This group or class, whose sense of security is purposefully undermined, is the target of terror. The purpose of this indirect method of combat is either to immobilize the target of terror in /09order to produce disorientation and/or compliance or to mobilize secondary targets of demands (e.g., a government) or targets of attention (e.g., public opinion) to change their attitude or behaviour favouring the short or long- term interests of the users of this method of combat [4].

The author did not consider non-human targets such as a database, critical national information infrastructure or other key public assets like petroleum pipeline etc. These are key targets of terrorist attacks as being witnessed in the Niger Delta area pre and post Federal government amnesty. The Niger Delta militants understand that by disrupting the economic nerve of the country, it would get the attention of the government and international organisations since its activities has local and international dimensions. Another point of disputation with this definition is the common class characters of victims. The Boko Haram insurgents have disproved this point. While Hamas targets Israelis, one cannot categorise the targets of Boko Haram. They attack Christians, Muslims, Shiites, Sunnis, children and adults. They attack in Cameroun, Chad and Nigeria. This irrationality is what has made the group tick.

The US State Department defines terrorism as the *premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents, usually, intended to influence an audience* [5].

Like Schmid's definition, this description fails to consider attacks directed against property. Maybe to maintain political correctness it ascribes terrorists' intents only to political motives. This is far from complete. Terrorists strike for political, religious, economic and other ideological motives. The definition also omits to mention acts of terrorism that are carried out by a government against its own people, or persons within its control. The current crisis in Syria is an example of government sponsored genocide against its own people.

Lord Carlile Berriew QC was appointed as an independent reviewer with the specific assignment of defining terrorism [6]. He reviewed legislative and academic definitions from scores of countries and writers. Some are mentioned below. He submitted-
Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination – the direct targets of violence are not the main targets [7].

This definition is in essence trying to classify common criminals as terrorists. Violent crimes are sufficiently dealt with by our criminal laws, but terrorism is of wider essence than regular crimes. Furthermore, this is more of a description of characteristics than a definition of the term.

The UN Resolution 1566 [2004] is one of the widest accepted definitions of terrorism. It has been adopted by many countries with mild variations.

Acts of terrorism are 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 organisation to do or to 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…

Like most other definitions non-human targets where not put into consideration in this description.

The US Federal Bureau of Investigation defined international terrorism thus:
International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum [8].

Some authors have settled for describing terrorism rather than defining it.

Paul Wilkinson said it is a *"weapon of coercive intimidation designed to make established authority and governments to submit to demands [9]".*

Bruce Hoffman summarised the character traits of terrorism, when he stated that acts of terrorism are-

- Ineluctably political in aims and motives;
- Violent, (or equally important, threatens violence);
- designed to have far-reaching psychological repercussions beyond the immediate victim or target;
- conducted by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia); and
- perpetrated by a sub-national group or non-state entity (but could be sponsored by nations- state sponsored terrorism) [10].

If defining terrorism could be so problematic, how then shall we define cyber terrorism? It is noted that one of the gaps in most definitions of terrorism is the absence of reference to non-human targets in terrorist acts. Defining cyber-terrorism must of necessity fill this gap.

The FBI, again, defined cyber terrorism as *the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against non-combatant targets by sub-national groups and clandestine agents.*

Professor Dorothy Denning defined cyber terrorism thus-
Cyber-terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, net-works and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at

least cause enough harm to generate fear. 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 non-essential services or that are mainly a costly nuisance would not [11].

Statutory definition of cyber terrorism in Nigeria can be gotten by a combined reading of Section 18. (1) of the Cybercrimes Act 2015 and section 1(2) of the Terrorism Prevention Act of 2011.

Section 18. (1) of the Cybercrimes Act 2015 says- *Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.*

Section 1(2) of the Terrorism Prevention Act of 2011 is rendered thus-
(2) In this section, "act of terrorism" means an act which is deliberately done with malice, aforethought and which:
(a) may seriously harm or damage a country or an international organization;
(b) is intended or can reasonably be regarded as having been intended to—
(i) unduly compel a government or international organization to perform or abstain from performing any act;
(ii) seriously intimidate a population;
(iii) seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization; or
(iv) otherwise influence such government or international organization by intimidation or coercion…

From the foregoing, cyber terrorism can be summarily defined as the illegal use of computer or computer network as a tool or target to deliberately harm, damage, unduly compel, seriously intimidate, destabilise or coerce a government or international organisation to do or refrain from doing a particular thing in furtherance of the terrorists' socio-economic, political or religious agenda [12].

Although a universal definition of terrorism is still far-fetched, there seems however to be a greater consensus on global terrorism standards. These standards include- violence or the threat of violence [13], people or property [14], audience [15], message [16], motivation [17], fear factor [18] Irrationality [19].

Some authors opine that terrorism standards cannot be applied to cyber-terrorism strictly, because cyber-attacks usually transcend national boundaries and it does no direct harm to individuals [20].

Unlike conventional terrorism which may be a weapon of mass destruction or casualty, cyber-terrorism is usually a weapon of mass disruption. Weapons of mass disruption are weapons, or better put, terror tactics that aims at unhooking the socio-political and economic status quo of a society. Terrorists may disrupt the national elections by hacking into INEC voter register database; they can disrupt the banking system by hacking into and taking over the Bank Verification Number (BVN) platform. They can critically disrupt the national economy by cyber-jacking [21] the Treasury Single Account (TSA) software etc. For the cyber-terrorist, guns, bombs and knives are obsolete [22].

Historically, terrorist activities arise out of various causative factors. Identifying these factors is critical to addressing terrorism whether traditionally or through the cyberspace. They include- Suppression of rights e.g., anti-apartheid struggle in South Africa; fight for equality and fair treatment; propagation of a religious or political ideology e.g., Boko Haram v. Nigeria; loss of confidence in judicial and governmental avenues for dispute resolution; allegiance to a particular foreign group or cause; unresolved historical, sociological conflicts and dissimilarities e.g., MASSOB v. Nigeria; fight for pride- to hurt the behemoth- Al-Qaida v. USA; gain sympathy and international audience- Palestine v. Israel.

The African National Congress of South Africa during the apartheid regime resorted to guerrilla tactics when it discovered its civil

engagement method was not gaining traction. Major infrastructure was targeted and destroyed. The terrorists justified their action as being a fight for freedom. Oppressive regimes have faced these kinds of opposition at one time or the other. Many modern terrorist organisations have religious colouration. Boko Haram, ISIS, LRA etc. all claim to be furthering the cause of Islam or Christianity through their violent activities.

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

It is necessary to understand the implication and ramification of Critical National Information Infrastructure (CNII). Section 3 (1) of the Cybercrime Act empowers the President, on the recommendation of the National Security Adviser to designate certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital in Nigeria, that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure. This designation takes effect only upon being gazetted.

What constitutes critical national assets or sector varies depending on the peculiarities of the countries or region involved. Sectors such as- Power and Energy, ICT, Health, Finance, Transport, Chemical and Biotechnology, nuclear etc. have been so designated. The European Union (EU) for example designated eleven sectors [23].

The efforts of the drafters of the National Cyber-security Policy (NCP) [24] must be commended for giving Nigeria a document we can work with. The NCP identified fifteen (15) critical national sectors including communications, manufacturing, dams, defence, information technology, government facilities, chemicals, power and energy etc. [25]. It is however, important to distinguish between Critical National Infrastructure (CNI) and Critical National Information Infrastructure (CNII). The focus of this paper is on CNII.

The nature and components of a CNII includes-

a) Computer systems, cyber networks or traffic data.
b) The infrastructure has been formally designated as a critical infrastructure.
c) The infrastructure is vital to Nigeria.
d) Incapacity or destruction of the CNII would affect security, public health and safety or any of its combination.

Some information infrastructure considered be critical to Nigeria include- Nigcomsat control centre; Galaxy Backbone providing data service to all Federal Government Agencies; Tier 3 data centres, intercontinental data cable providing internet to Nigeria, private telecoms operators infrastructure, Transmission Company of Nigeria control centre and base stations, internet exchange points etc.

The first issue to be addressed in a national anti-cyber-terrorism strategy is the designation of critical national infrastructure. This is not a walk-in-the-park assignment that could be dictated by a smart administrator ensconced in his cosy office. It takes a lot of technical, legal and administrative input from all stakeholders. To designate infrastructure as critical to the nation, it is best to identify our most critical sectors.

MANIFESTATIONS OF CYBER-TERRORISM

1. Illegal Access to a Computer System or Network

Section 8 of the Cybercrimes Act 2015 provides-

Any person who without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment.

The technical name for this offence is hacking. Hacking is simply an act of securing unauthorised access to a computer or computer network. Sections 385-389 of the Criminal Law of Lagos State 2011 is analogous to this section. The main tool of cyber-terrorists is to obtain unauthorised access to the computer system of another.

Hackers are divided into white-hat hackers and black hat hackers. The first category is authorised to perform security functions while the black-hat hackers are unauthorised. Reference to 'hackers' hereinafter means Black-hat hackers. Hackers terrorise individuals, organisations and governments in various ways and means. including-

i. Code Hackers - They can succeed in making the computer do nearly anything they want. They can get access into the computer and therefore, use it for any sinister motive. Code hackers can cause substantial damage to reputation among other economic havocs.
ii. Crackers- this group is very similar to code hackers. Their pleasure is to 'disgrace' so called secured systems.
iii. Cyberpunks- they have mastered the art of cryptography. They can decode digital signatures and other security devices mounted on a system. This gives them unhindered access to such sites to steal, destroy or modify programmes to further their sinister motive.
iv. Phreakers- they use the internet to wreak havoc on the telecommunication system like telephone, GSM, Digital TV etc. [26].

It must be stated that not all illegal access to a computer system amounts to cyber terrorism. The cyber-terrorist is an ideologue that is out on a higher purpose than mere immediate pecuniary gain. Hackers, except for some who are out on revenge mission, are usually criminals-for-hire. They can be employed or converted by terrorists to help implement a cyber-terrorism master-plan.

2. Virus Attack

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document [27]. Section 16 of the Cyber Crime Act makes unauthorized modification of computer data a crime. The section is rendered as follows-

16. (1) Any person who with intent and without lawful authority directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than N7,000,000.00 or to both such fine and imprisonment.

(2) For the purpose of this section, a modification of any data held in any computer system or network includes modifications that take place whereby the operation of any function of the computer system or network concerned, or any-

(a) program or data held in it is altered or erased;

(b) program or data are added to or removed from any program or data held in it;

(c) program or data are suppressed to prevent or terminate the availability of the data or function to its authorized users; or

(d) act occurs which impairs the normal operation of any computer, computer system or network concerned.

Virus attack combines with hacking to constitute the most lethal weapon of the cyber-terrorist. If a virus is designed to avoid detection by the anti-virus system in the target computer, the program or data can be easily altered, erased, suppressed or impaired. The implication of virus attack on critical information infrastructure is huge. Monies and efforts spent on election information management, cloud-based data, national biometric database, e-governance infrastructure, control centres of major national assets could easily go down the drain with a single virus attack.

Other means of cyber-terrorist attacks in this class include Trojan Horses [28], Logic Bombs [29], Denial of Service Attack (DoS) [30], Worms [31].

3. Invasion of Privacy

Another tool of cyber-terrorism is the illegal use of private information to hold people to ransom. The question any inquirer may ask is what has privacy got to do with terrorism? The Snowden case caused massive international relations disruption. Snowden as a former contractor to the CIA divulged highly sensitive information on how the US was invading the privacy of other countries contrary to international norms and decorum. This is a template for emerging cyber-terrorist manipulation.

By engaging many more 'Snowdens', terrorists can create sufficient distrust among international allies sufficient to weaken their resolve or break up their cooperation. This gives room to terrorists to hold the ace and take heinous initiatives without restraint.

Section 37 of the 1999 constitution of Nigeria guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. Privacy in the information age has been described as the rightful claim of the individual to determine the extent to which he wishes to share of himself with others. It means the individual's right to control dissemination of information about himself [32].

A cyber-terrorist need not hack into the computer system or use any form of virus attack to hurt a nation or key national or organisational stakeholders, all he needs to do is to 'harvest' publicly and remotely held information to achieve his devious purpose. Here is a scenario of how this could be done- Gen. AB of DPP party is a retired army general who is running his campaign on the promise to secure Nigeria against terrorists, reflate the economy and improve infrastructure.

Terrorists having studied the backgrounds of the other candidates, realise electoral victory by Gen. AB would lead to their decimation. They therefore, decide to run social media campaigns projecting the general's confidential health information about his impotence, claiming that the children who bear his name were actually adopted. This information was gotten from the Army Health Service which recently digitised the health information of past and present officers to modernise its medical records. A terrorist who works at the medical records office got the information and passed it to his organisation. This information was primed till it became a national scandal forcing the General to withdraw from the race. This no doubt is a veiled terrorist hatchet job that could be easily perfected and acted upon by many people.

Another variant of invasion of privacy is when private mass e-mail and SMS message is sent to people whose information had been garnered from telecommunications service providers or other mediums. Terrorists can use this medium to set off sectarian crises. For example, a phantom message reads:

BROTHERS AND SISTERS, THE CATHOLIC CHURCH IN SABON GORO OF KUCHIGORO LOCAL GOVERNMENT, ABUJA HAS JUST BEEN BURNT DOWN BY MUSLIM YOUTHS LED BY THE CHIEF IMAM OF KUCHIGORO. OVER 120 MEN, WOMEN AND CHILDREN HAVE BEEN KILLED. PLEASE RISE UP AND START SLAUGHTERING ANY NORTHERN MUSLIM AROUND YOU!

NB: YOU WILL NOT HEAR THIS FROM THE MAIN NEWS OR SOCIAL MEDIA AS THE GOVERNMENT HAS SUCCEEDED IN BUYING THEM ALL OVER.

This message is a trap which many gullible people can fall into to help terrorists fulfil their purpose. A dispassionate assessment of the information would reveal patent flaws, as there is no Kuchigoro Local Government in Abuja, neither is there any Catholic church burnt. The dimensions of destruction possible through cyber-terrorism are almost endless. This is a wake-up call to the nation to quickly prepare to prevent such possibilities.

STUXNET: A MODEL CYBER-TERRORIST ATTACK

Stuxnet attack was a ground-breaking event in the field of cyber security. The incident transmuted an industrial scale cyber-attack from a mere hypothetical scenario into reality. The attack further revealed the level of

sophistication a cyber-attack must have to achieve its goal of terror, death and huge socio-economic dislocation. Stuxnet was discovered in June 2010, it set the whole IT security sector in frenzy, trying to understand the phenomenal malware. Prof. Thomas M. Chen summarised the technical details of the attack in his monograph *Cyber-terrorism After Stuxnet* [33]. It will suffice to state for our purpose in this paper that the malware was very large (about 500 kilobytes) and very complicated in configuration. The erudite Professor gave some relevant details which is herein summarised.

The most probable means of infection is through a removable flash drive, because the target of the attack, as expected, was not internet connected. Stuxnet exploited vulnerabilities in Windows PC and took advantage of the hard-coded default password in Siemens Simatic WinCC software (CVE-2010-2772) which allowed access to the back-end data-base. Once injected into the database, Stuxnet infects the PC running the WinCC database.

What made Stuxnet lethal was the fact that its writers had perfect knowledge of the target. Stuxnet is interested only in Siemens Simatic S7 PLCs (programmable logic controller), which are programmed by Windows PCs running Simatic Step 7 software. After Stuxnet infects a PC running Simatic Step 7, it will then load its own malicious blocks into a connected Simatic S7 PLC.

The complexity of the malware and its elaborate nature of the operation suggests that the operators had the support of state actors to achieve the deployment of Stuxnet. The intent of the attackers was multiple-layered- Slow down the Iranian nuclear acquisition capability, completely destroy the programme and foreclose future interest in such high impact project. Another possible intent is to use this as a test case for the sale of cyber protective solutions to willing buyers.

DO YOU WANNA CRY?

On Friday 12th May, 2017, over a 100,000 organisations in about 150 countries [34] woke up to a nightmare, their valuable information could no longer be accessed, it has been held hostage! The message on their computer screens said, *ooops, your files have been encrypted* [35] the page shows a chilling message to the victim, informing him/her of the encryption of messages in the computer, a countdown timer to when payment must be raised and when files will be lost, is shown. The Bitcoin wallet account of the ***Info nappers*** [36] with the ransom amount is placed conspicuously on the page. The ransomware is programmed to encrypt almost all types of files. Over 149 types of files have been listed including but not limited to .ppsx, .ppt, .pptm, .java, .jpeg, .jpg, .mp4, .mpeg etc. [37].

The question a lot of people have asked is how did we come about this ransom ware? According to the Chief Legal Officer of Microsoft, Brad Smith-

This attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem… And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today — nation-state action and organized criminal action [38].

The National Security Agency (NSA) of the US had been stockpiling vulnerabilities in the Windows operating system for some time, this fell into the hands of the wrong people thereby causing a cataclysmic impact on the world.

A look at the Cybercrimes Act 2015 shows that the Act envisages this type of criminal/terrorist activity. Section 8 of the Act provides for Systems Interference. It is rendered thus:

8. Any person who without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to

imprisonment for a term of not more than 2

Source: Hackread [39].

years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment.

The operative words in the ransomware context are *damaging, deleting or suppressing computer data.*

Section 16 of the Act further strengthens the argument by highlighting what modification entails

(2) For the purpose of this section, a modification of any data held in any computer system or network includes modifications that takes place whereby the operation of any function of the computer system or network concerned, or any-

(a) program or data held in it is altered or erased;

(b) program or data are added to or removed from any program or data held in it;

(c) program or data are suppressed to prevent or terminate the availability of the data or function to its authorized users; or

(d) act occurs which impairs the normal operation of any computer, computer system or network concerned.

Section 16 (2c) hits the bull's eye. The elements to be proved by the prosecutor would include- suppression of data; prevention from availability; termination of availability to authorised users.

Some legal and regulatory issues arise from this incident which needs further exposition outside of this paper. NITDA under its mandate in Section 6(f) of the NITDA act has a duty to provide up-to-date advise to all security and non-security agencies of the government including private sector participants on security architecture to be deployed in the protection of cyber assets. Some issues to be looked at include encryption standards, PKI etc.

If a software provider makes an update on its service and such was not accepted by the user leading to security breach and loss, who is liable? The court in this instance would consider the terms and conditions for the

software, the opportunity the user had to upgrade, the ease of use of the newly updated software among others. In this regard, it is essential for NITDA to review the terms and conditions of the software service providers or provide guidelines to ensure IT service consumers are well protected. Another issue that the Wannacry incident raises is the obligation to report to the Nigerian Cyber Emergency Response Team (Ng. CERT) according to section 21 of the Cybercrimes Act (2015). The Ng. CERT and NITDA must improve communication on this issue, due to its impact on national security.

In addition to other necessary advisories NITDA must issue to Nigerians and Federal MDAs in particular, offline back up and, or secured cloud back up of critical national information must become mandatory in order to reduce the effect of future ransom ware attacks.

LEGAL FRAMEWORK FOR TACKLING CYBER-TERRORISM IN NIGERIA

In a civilised society, actions must be based on the rule of law. A lack of well-thought legislative and policy direction can as well make us kiss goodbye to any dream of winning the war against cyber-terrorism.

The Terrorism (Prevention) Act, 2011 expressly prohibits acts of terrorism. An "act of terrorism" means an act which is deliberately done with malice, aforethought which may seriously harm or damage a country or an international organization; intended or can reasonably be regarded as having been intended to— unduly compel a government or international organization to perform or abstain from performing any act; seriously intimidate a population; seriously destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization; or otherwise influence such government or international organization by intimidation or coercion; and involves or causes, as the case may be- an attack upon a person's life which may cause serious bodily harm or death; kidnapping of a person; destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property, likely to endanger human life or result in major economic loss; the seizure of an aircraft, ship or other means of public or goods transport and diversion or the use of such means of transportation for any of the purpose of causing terror; the manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of biological and chemical weapons without lawful authority etc. [40].

The Act does not distinguish between traditional and cyber-terrorism because, terrorism can be carried out by whatever means, the end result is the same- sorrows, tears and blood [41].

The Act further empowers security agents and bank officials to report, seize and arrest persons connected with transfer or receipt of money suspected to be meant for terrorism [42]. It also provides for how to deal with terrorist properties [43]. Procedure and other relevant provisions are also made to adequately address terrorism in Nigeria.

Section 15 of the Money Laundering Act 2011 prohibits the laundering of money for the purpose of terrorism or terrorist financing. Convicted persons are liable to 5 to 10 years imprisonment without option of fine.

Section 18 of the Cybercrimes Act 2015 is most apt to our discussion here; it is rendered as follows-

18. (1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.

(2) For the purpose of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended.

Only the Cybercrimes Act recognises the power of the computer in furthering terrorist activities, also, only the Act allows a sentence

of life imprisonment for a convict. The practical implication of this is that terrorists could be charged under both the Terrorism Prevention Act and Cybercrimes Act if there is evidence of the use of any computer or cyber infrastructure. While the TPA gives more legroom for the prosecutor, the Cybercrime Act gives an appropriate sentence for terrorism.

The recent hoopla over the fine imposed on MTN Nigeria for not complying with Nigerian Communications Commission (NCC) regulation on the Registration of Telecoms Subscribers is worth mentioning here. Section 71 of the Nigerian Communications Act which established the NCC empowers it to make regulations for the effective administration of the communications sector. It was in furtherance of this provision that the above mentioned regulation was made. The Nigerian authorities argued that the insipidity of MTN in complying with this directive fuelled the Boko Haram carnage in North East Nigeria [44]. This author's take-away from the fiasco is that Compliance officers and advisers to companies must understand the prime place of technology regulation and use in modern business. If not properly handled, MTN's multi-trillion Naira investment in Nigeria may go down the drain.

SUGGESTED POLICY OPTIONS

In view of the foregoing, certain policy options must be considered in foiling a cyber-terror attack or mitigating the effects. They include-

i. Immediate convening of a national stakeholders conference by Office of the National Security Adviser on designation of critical national information infrastructure pursuant to section 3 of the Cybercrimes Act 2015. The list in Paragraph 7.5 of the National Cybersecurity Policy is sectorial; this does not meet the requirements of the Act.
ii. A national action plan coordinated by NITDA that critical national data should be stored in Nigeria and regulated by Nigerian law to reduce possibility of foreigners access and security compromise.
iii. The Nigerian Army, State Security Service, Police and other security agencies should be trained on cyber-security management.
iv. A scheme can be devised to employ technology savvy youths who can act as the nation's 'cyber-army'. This falls in line with NITDA's strategy on Digital Jobs Creation.
v. The National Cyber Security Policy and Strategy implementation should be expedited and well-funded to achieve the desired objectives.
vi. NITDA should work with public and private stakeholders to set a National Information Technology Infrastructure (NITI) Guideline.
vii. Staff of NITDA, IT staff of MDAs and security agencies must be properly debriefed of all codes and access rights to the computer and automated systems of the employer in compliance with Section 31 of the Cybercrimes Act.
viii. Our tertiary institutions should be funded to establish cyber-security research centres to train manpower, monitor cyber-security developments, detect cyber-terror attack, advise stakeholders and activate cyber-security actions when necessary.

CONCLUSION

Nigeria as a heterogeneous conglomeration of diverse interests has long lived in the shadow of internal combustion. As long as the unresolved issues fester, cyber-guerrilla tactics cannot be ruled out in the present and the future. There needs to be a coordinated national response to the gorgon of cyber-terrorism, no single agency has all the solutions all hands must be on deck and in sync to avert, contain and control future attacks.

REFERENCES

1. www.merriam-webster.com accessed on 6th July, 2017.
2. Cyberlaw S. 1.01, at 1–3 (2001). Cited in *Blacks Law Dictionary*, Bryan A Garner (ed) (8th Edition, 2004).
3. Tucker D, *Skirmishes at the Edge of Empire* (Praeger, Westport, 1997, 51p).
4. Alex P. Schmid, *Political Terrorism: A Research Guide to Concepts, Theories, Data Bases and Literature* (Amsterdam: North Holland Publishing, 1983), 91.

More recently, Schmid has revised his definition of terrorism to include a social science and a legal version. For more information, see Alex P. Schmid, "Terrorism and the Use of Weapons of Mass Destruction: From Where the Risk?," *Terrorism and Political Violence* (Winter 1999); 11(4): 128–129p. [endnote 18] and Alex P. Schmid, "The Problems of Defining Terrorism," in Martha Crenshaw and John Pimlott, eds., Encyclopedia of World Terrorism (Armonk: M.E. Sharp, 1997), 21–22p.

5. U.S. State Department, Patterns of Global Terrorism 1999 (April 2000), available from http://www.state.gov/www/global/terrorism/1999report/intro.html; Internet. The report states, "The term 'non-combatant' is interpreted to include, in addition to civilians, military personnel who at the time of the incident are unarmed or not on duty." Also considered are "attacks on military installations or on armed military personnel when a state of military hostilities does not exist at the site."
6. The Definition of Terrorism a report by Lord Carlile of Berriew Q.C. Independent Reviewer of Terrorism Legislation (Commissioned by Home Affairs Office March 2007).
7. Schmid A and Jongman A; *Political Terrorism* (North-Holland, Amsterdam,1987).
8. U.S. Department of Justice, Federal Bureau of Investigation, Terrorism in the United States 1998, available from: http://www.fbi.gov/publications/terror/terror98.pdf; Internet, i.
9. Paul Wilkinson, *Terrorism versus Democracy*, The Liberal State Response (London: Frank Cass Publishers 2nd Ed. 2006), 12
10. Bruce Hoffman *Inside Terrorism* (Columbia University Press, 2006).
11. Dorothy Denning, "Cyberterrorism—Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives," Washington, DC: U.S. House of Representatives, May 23, 2000, available from www. stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf.
12. Femi Daniel 'Cyber Terrorism: Need of a New Kind of Army' *The Nation* (Lagos, 1 March 2016).
13. The Websters Law Dictionary defines violence as the use of physical force, especially physical force utilized with malice and/or the attempt to harm someone. Violence or a threat of it is what creates the sense of siege that the terrorist exploit for their nefarious activities.
14. A class of people or residents within a geographic expression, and recently certain strategic or symbolic properties are the targets of terrorists.
15. The audience the terrorists hope to reach are beyond the targets of terror. It may be local or international media, government, international organisations etc. it is because terrorists cannot easily deal with the actual audience that is why they go for 'soft targets'. When the Palestine Liberation Organisation's Black September Organization took Israeli athletes hostage during the 1972 Munich Olympic Games, its intended target audience was the leaders of various countries, including Israel and Germany, and the entire international community as a whole.
16. Every terrorist act is an expression of an over-arching message intended by the terrorist for a target audience. Immediately after September 11 attacks, Osama bin Laden announced that his Al- Qaida organisation is responsible and that the act was to punish America for interfering in the domestic affairs of Muslim countries among others. Boko Haram's message got very clear after the Chibok girls kidnap when the girls where shown wearing hijab and reciting Quranic verses. The terrorists insist that Western education is sin and they were out to wipe out all western influence in their domain including Christianity and western education.
17. For an act of violence to be considered terrorism, it must be politically, ideologically, socially, or religiously

motivated. This motivation can be a combination of two or more factors. This critically differentiates terrorism from mere criminal violence.

18. The essence of terror is the instillation of fear. Although a consensus on the definition of terrorism is still being sought, however, what words cannot express, is fully felt and known when one sees it. A terrorised people are under a state of economic, political, social and religious siege. Activities are altered and fear rules the community in place of freedom.
19. This is also referred to as *extra normality.* Terrorists engage in abnormal and irrational behaviours. It took long for the world to understand why terrorists like Lord's Resistance Army would engage child-soldiers. Many also wonder how a lady carrying bomb beneath her *burqa* would blow herself to pieces. These irrational actions define most terrorist organisations.
20. Jerrold M. Post, Kevin G. Ruby, Eric D. Shaw, From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism, *Terrorism and Political Violence*. (Summer 2000); 12(2): 97–122p.
21. The cyber parallel of hijacking.
22. Femi Daniel *Cyber-crimes: Obsoleting the Guns, Bombs and Knives* (NLSJ No. 1, 2010), 46–56p.
23. They are i. Energy ii. Information, Communication Technologies (ICT) iii. Water iv. Food v. Health vi. Financial vii. Public & Legal Order and Safety viii. Civil Administration ix. Transport x. Chemical and Nuclear Industry xi. Space and Research see article by Femi Daniel http://thenationonlineng.net/cyber-terrorism-need-of-new-kind-of-army/ accessed on 25th January, 2018
24. Launched in February 2015 as part of the three cyber security documents launched on the same day. The other two are National Cyber-security Strategy and Cybercrimes Act 2015.
25. Others are commercial facilities, financial services, food and agriculture, emergency services, transportation, public health, water and waste.
26. Dr. Gupta and Agrawal *Cyberlaws* (India: Premier Publishing Company, 2016) 64
27. https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html accessed on 25th January, 2018
28. These, unlike viruses do not usually replicate themselves; instead they hide their true intent behind something benign. They can present themselves as games, programs, screensavers etc. Trojan horses are designed primarily to give hackers remote control of the victim's computer. It also engages in some other sinister acts like sending itself to every contact on the victim's address book; erase or alter the victim's files; steal credit card details; install a virus or download other unwanted programs etc.
29. These are malicious programmes that are primed to start operating at a specified time in the future. The trigger could be time or event specific. Some original software makers could insert this programme in their software to make it start malfunctioning after some years in order to increase purchase of the programme. A sacked or maltreated employee may also want to hurt the employee and therefore programme a logic bomb into the system to disrupt the operations of the organisation at a future date without being directly linked with the incident.
30. This is a deliberate, malicious flooding of electronic traffic of commercial or 'high-value' websites in a bid to prevent legitimate traffic, disrupt connection, prevent access to service by a client or prevent service to the client
31. Worm is a standalone malware computer programme that replicates itself in order to spread to other computers. Unlike a virus, it does not attach itself to an existing program. Worms almost always cause at least some harm to the network even if only by consuming bandwidth
32. Adam C. Breckenridge, *The Right to Privacy*, cited in Talat Fatima: *Cybercrimes* (Eastern Book Company: 2011) 171p.
33. Thomas M. Chen: *Cyber-terrorism After Stuxnet* Prepared for the US Army War

College Strategic Studies Institute (June 2014).
34. http://technology.inquirer.net/62619/least-100000-groups-150-countries-hit-ransomware accessed on 11th July, 2017.
35. http://www.dailymail.co.uk/sciencetech/article-4518538/Cyber-attackers-WannaCry-send-eerie-new-message.html accessed on 11th July, 2017.
36. My revision of the word- kidnappers in the context of information technology and cyberspace
37. http://bgr.com/2017/05/15/wanna-cry-ransomware-virus-windows-wannacry-explainer/ accessed on 11th July, 2017.
38. http://www.latimes.com/world/europe/la-fg-europe-computer-virus-20170514-story.html accessed on 11th July, 2017.
39. https://www.hackread.com/wannacry-ransomware-attackers-new-message/ accessed 28th July, 2017.
40. Section 1 (2) of the Terrorism (Prevention) Act 2011.
41. Apologies to the late Fela Anikulapo Kuti the legendary musician who popularised this expression.
42. Section 13 TPA 2011
43. Sections 15, 16 and 17 TPA 2011
44. Tobi Soniyi, Omololu Ogunmade, Damilola Oyedele, MTN fuelled Boko Haram Insurgency, www.thisdaylive.com of 9th March, 2016.

Cite this Article
Isa Ali Ibrahim Pantami & Femi Daniel Cyber-Terrorism: Legal and Policy Options for Coordinated National Preparedness. *National Journal of Cyber Security Law*. 2018; 1(1): 1–14p.