Draft Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference

CYBERCRIME AND CYBER SECURITY AS CHALLENGES TO THE FIGHT AGAINST GLOBAL TERRORISM

Prof. T. I. Akomolede*
Dr. B. O. Jemilohun**
Mr. M. S. Afolayan ***

Introduction

Humanity is known to have witnessed two great technology-based revolutions; the industrial revolution and the information communication technology revolution.\(^1\) However, much as the industrial revolution brought positive developments to humanity, the advent of the information communication technology age did not come without some challenges. Some of these challenges are mainly based on the wrongful use of computers or the deployment of the computer on the internet for criminal purposes.

It is common knowledge that the internet is one of the fastest-growing areas of technical infrastructural development. The ubiquity of the internet is noticed everywhere by the fact that information communication technologies are omnipresent and there is a massive trend towards digitization. Presently,\(^2\) there are about 6 billion internet users\(^3\) in the world, up from the 2 billion users in 2011.\(^4\) In the African continent alone, there are over 1.1 billion internet users with a penetration of 28.6% of the total population.\(^5\)

The growing functionality and ease of computerised networks however come at a price. As businesses and societies in general rely increasingly on computers and internet based networking, cybercrime and other attacks on digital operations have increased around the world. Beyond this misuse of the internet by the abuse of private and personal information for financial gain and other malicious intentions, cyber criminals have learnt to steal national information, attack critical national information infrastructures, commit acts of cyber terrorism by disrupting traffic, infect whole networks with malicious software like worms and botnets, and generally commit criminal acts of international magnitude.

This paper takes a look at cyberspace as a non-physical realm, the challenges of securing it and the operators therein from the lawlessness being witnessed presently in the form of cybercrimes and at a more dangerous level, global terrorism. The great virtues of the internet – ease of access, lack of regulation or centralised oversight, vast potential audiences and fast flow of information at little or no cost have been turned to the advantage of clandestine groups who have the sole aim of terrorizing society. As at present, virtually all the active terrorist groups

---


\(^2\) As at November 2015

\(^3\) Internet World Stats – Africa Internet Users November 2015 available at [www.internetworldstats.com/stats1.htm](http://www.internetworldstats.com/stats1.htm) accessed on 21/04/2016


\(^5\) Footnote 4 above
Draft Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference

have established one form of presence or another on the internet as there are presently hundreds of websites serving terrorists and their supporters.  

The paper also attempts to look at the one or two legal responses both from the national level and a regional level and some attempts made at the global level to bring the challenge of global terrorism through cybercrime under control. The paper concludes by making some suggestions and lending its voice to the need for a global cyberspace treaty, not just to stop terrorism but to secure cyberspace for personal, commercial and national use.

Cyberspace: The Phenomenon and the Operations

Cyberspace refers to the boundless space sometimes referred to as the internet. It refers to the interdependent network of information technology components that underpin many of our communication technologies in place today. In a broader sense, it comprises information communication technology networks, computer resources and all the fixed and mobile devices connected to the global internet. These may be connected through undersea cables, satellites in outer space, land lines and radio links. The cyberspace of any nation is an integral part of the global cyberspace and it cannot be isolated to define its boundaries since cyberspace is borderless.

Cyberspace has become the terminology for that invisible realm between two computers or between two smart-phones that may be physically located within the same building or thousands of miles apart. As a social experience, individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, and engage in political discussion, using this global network. The term has become a conventional means to describe anything associated with the internet and the diverse Internet culture. Thus, according to Morningstar and Farmer (2003), cyberspace is defined more by the social interactions involved rather than by its technical implementation.

Unlike the physical world that is limited by geographical boundaries—land, sea, river waters and air—cyberspace can and is continuing to expand. Technology innovations are pushing the speeds of communication and computing to new limits; quantum computers promise to far exceed Moore’s Law, which predicts that the processing power of computers doubles every

7 The term cyberspace was made popular by Gibson, W., (1984) Neuromancer, Ace Books, New York. p.69 (1984) in the sci-fi novel of the same name and it has since come to mean any non-physical terrain created by online computer systems.
eighteen months. Increased Internet penetration is leading to the rapid growth of cyberspace, since the size of cyberspace is proportional to the activities that are carried through it. Among those activities: the exchange of goods or services, financial transactions through banks, credit card payments, email communications, social networking, exchange of pictures, videos or music. These activities lead to the seamless merging of cyberspace with the physical world.

From the security angle, the US Department of Defense (DoD) defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” The DoD advised that it would use the definition till further notice, which statement is seen as an acknowledgement of the rapid evolving nature of the field. The definition also nullified the definition contained in 2006 National Military Strategy for Cyberspace Operations.

Kramer at al (2009) went beyond the DOD’s definition and conceived cyberspace as a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies. In the view of the authors, these interdependent and interconnected information networks and systems reside simultaneously in both physical and virtual space and within and outside of geographical boundaries.

The dwellers in cyberspace that make use of these independent and interconnected networks vary from entire nation states and their component organizational elements and communities down to lone individuals and amorphous transnational groups who may not profess any allegiance to any traditional organization or national entity.

Cyber is one of the most frequent used terms in international security discussions today. It is definitely a term of increasing importance in the lexicon of most international lawyers and security experts as it has moved from the domain of the geeks and the nerds to that of everyday use. However, laws, criminal justice systems and international cooperation have not kept pace with technological change. Not all countries have adequate laws to address issues emanating from cyberspace and of the ones that have laws, resolving all the legal, enforcement and prevention problems is still a long journey.

**Cybercrime: The Concept and its multi-facets**

---

15 Supra, note 12 above
18 Ibid.
19 At page 28
Draft Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference

Cybercrime as a phenomenon is a subject hard of precise definition. It may refer to the series of organised crime attacking both cyber space and cyber security. Sophisticated cyber criminals and nation states among others present risks to our economy and national security. Cybercrime as a concept has become a nebulous phenomenon, and it seems there is no generally accepted definition for it yet.

In the opinion of Groebel, J. et al (2001), "given both the novel nature of the Internet and the subsequent growth of traditional crimes that exploit ICT as well as new crimes, which have grown in parallel to technological developments in the communications sector, it is unsurprising that a standard universal definition of cybercrime has not yet evolved".22 Even the United Nations Manual on the Prevention and Control of Computer-related Crime23 does not have a ready definition for cybercrime. It merely states that “computer crime can involve activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may or be criminal as well”.

The word ‘cybercrime’ may not be found in a contemporary lexicon, but it is a very popular term describing the criminal activities related to cyberspace. As pointed out above, there appears to be no scholarly consensus on a single definition of the concept, but it appears as if writers and law drafters are more comfortable with describing various elements constituting cybercrime than defining it.24 For instance, according to the Council of Europe Convention on Cybercrime, cybercrime involves ‘action directed against the confidentiality, integrity and availability of computer systems, networks and data...”25

Odumesi (2014) defines cybercrime as a crime involving the abuse or misuse of digital resources in a cyber environment on or through the internet, computer networks, computer systems and wireless communication systems.26 Again, Cybercrimes may be seen as means of unauthorized interception of computer systems and computer data through computers with intent to intercept the network and computer systems, in order to obtain personal data or manipulate with these data, use of computer resources for terrorism, intercept and obtain data from computer systems for financial, political and blackmailing purposes, unlawful hindrance of computer systems, acts against confidentiality, integrity and availability of the computer system data.27

---

23 Footnote 19 above.
Draft Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference

The first major instance of cybercrime was reported in 2000, when a mass-mailed computer virus affected nearly 45 million computer users worldwide. Today, the internet is awash with news of all manners of criminal behaviours that are perpetrated in Cyberspace.

**Manifestations of Cybercrime**

Cybercrime is manifested in various illegal deployments of information communication technology infrastructure. The loss to private individuals, businesses and nations has reached such high levels that it is considered one of the main threats to national security in the 21st Century. Cybercrime manifests in various forms as: hacking, cyber theft, installation of virus and worms, spamming, identity theft, cyber harassment, cyber laundering, website cloning, online fraud, cyber stalking etc.

Cybercrime ranges across a spectrum of activities. At one end are crimes that in involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained information to blackmail a firm or individual and the growing crime of identity theft. Midway along lie transaction based crimes such as fraud, digital piracy, money laundering and counterfeiting. At the other end of the spectrum are those crimes that attempt to disrupt the actual working of the internet – that is the use of the internet to cause public disturbances or even death.

Cybercrime is a multi-dimensional and global phenomenon that blurs the traditional distinction between the threats to internal and external security and does not respond to single jurisdiction approaches to policing. It is interesting to note that a recent study on cybercrime by the UNODC observed that as the world moves into a hyper-connected society with universal internet access, it is hard to imagine any crime that will not involve electronic evidence linked with internet connectivity.

The report further reveals that globally, cybercrime acts show a broad distribution across financial-driven acts, and computer-content related acts, as well as against the confidentiality, integrity and accessibility of computer systems. Victimization survey also reveals an increase in cybercriminal activities such as online credit card fraud identity theft, unauthorised access to email account as compared to conventional crime forms like typical burglary, robbery or car theft.

**Cyber Security**

---

28 MessageLabs Intelligence: 2010 Annual Security Report, Symantec
32 Ibid
According to the ITU,\footnote{International Telecommunication Union (2012) Understanding Cybercrime: Phenomena, Challenges and Legal Response. Available at \url{http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf} accessed on 17th April, 2016.} cybercrime and cybersecurity are two issues that can hardly be separated in an interconnected environment. The fact that the United Nations General Assembly\footnote{UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.} resolution on Cybersecurity\footnote{Recommendation X .1205 Overview of Cybersecurity in ITU, List of Security-Related Terms and Definitions, available at: \url{www.itu.int/dms_pub/itu/oth/0A/0D/T0A0D00000A0002MSWE.doc}} addressed cybercrime as one major challenge underlines this.

The term “Cybersecurity” is used to summarise the various activities and the ITU in one of its recommendations\footnote{Footnote 33 above} suggests a definition, description of technologies and network protection principles.\footnote{ITU, List of Security-Related Terms and Definitions, available at: \url{www.itu.int/dms_pub/itu/oth/0A/0D/T0A0D00000A0002MSWE.doc}.} “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user’s assets. Organisation and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organisation and the user’s assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality.”\footnote{See further, the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009), 2007, available at: \url{www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programmedeveloping-countries.pdf}.}

Cybersecurity plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation’s security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.

The ITU opines further that, at the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.\footnote{See further, the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009), 2007, available at: \url{www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programmedeveloping-countries.pdf}.} Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime. The development and support of cybersecurity strategies are a vital element in the fight against cybercrime.
However, the legal, technical and institutional problems identified by the issue of cybersecurity are global and far-reaching and can only be tackled through a comprehensive strategy considering the role of different stakeholders and the existing efforts within a framework of international cooperation. Thinking along this line, the World Summit on the Information Society recognized the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime.

In other words, cyber security may be seen as the body of rules, technical competencies, and sensitization and awareness programmes put in place for the protection of cyberspace and the human beings that interact therein. This becomes essential because as we become more dependent on cyberspace, we undoubtedly face new risks.

**Terrorism: the Phenomenon.**

The search for a universal, precise definition of terrorism has been challenging for researchers and practitioners alike. Terrorism has been defined as “premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents, usually intended to influence an audience”. According to the Federal Bureau of Investigation, terrorism is “the unlawful use of force or violence against persons or property to intimidate or coerce government, the civilian population, or any segment thereof, in furtherance of political or social objectives”.

It is obvious that terrorism is not the problem of any singular nation and in the same vein; no singular nation can wage a successful war against terrorist activities. The dimensions of terrorism are global and thus global responses are required. This is why the United Nations has enacted several Conventions against terrorism. While individual nations have made laws to combat cybercrime with their territories, it is becoming more obvious that more than national legislation or regulation, concerted global efforts are required in the fight against cyber crime and the deployment of the internet for terrorist activities.

**The Concept of Cyber-terrorism**

Cyber criminals largely began their nefarious acts by committing petty crimes in different parts of the world with different motives in mind. But with developments in ICT and the advantages

---

40 The WSIS Tunis Agenda for the Information Society, is available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=22670
41 Section 2656f(d) United States Code of Federal Regulations Title 22 of the U.S. Code
Draft Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference

offered by the internet comparatively, criminality has graduated into terrorism. Sadly, there appears to be a convergence between cybercrime and terrorism. In the opinion of Bucci, cyber-terrorism is focused largely on western democracies because they are ripe targets in the sense that these countries are either highly dependent almost completely in some cases on cyber means for nearly every societal interaction, or are racing towards that goal.

But firstly, one may wish to differentiate between two major forms of cyber-terrorism. The first leg is the type of terrorism restricted or largely carried out in the online world. This is where terrorist activities take place only on the internet with no direct real life consequences. Here, one may have large scale disruption of computer networks, especially of personal computers connected to the Internet. Individuals, businesses and even countries (and here the closest example that comes to mind was the assault made on Estonia in 2007 where the highly developed network of a small country was temporarily brought to its knees) may be victims of these but there is no direct physical harm on people and physical infrastructures.

The other dimension comprises of the deployment of the various facilities on the internet by real terrorists who may not be technology savvy or have too much knowledge about how to disrupt functioning ICT systems, yet they can leverage their internet capabilities to carry out their missions for real world terrorist activities that may affect people who may not use the internet or have any online presence. This second aspect is what this paper has to deal with presently. Several online reports have shown that the wide possibilities of information communication technology in cyberspace is a cause for concern.

**Impact of the Internet on Terrorism**

Perhaps the most important characteristic is the ubiquity of the Internet. This means that internet connectivity is everywhere and accessible by or to almost everyone. As the internet serves, private, business, governmental and international needs, it also serves criminals. It essentially allows terrorist organizations to operate on a global basis without the added requirement for physical infrastructures and personnel. This is actually the biggest advantage terrorist organizations currently have since it allows them to communicate their message to decentralized cells around the world in efforts to ensure terrorist operations are conducted in support of the greater intent. It also allows them to establish successful information operation campaigns against the U.S. and its allies through the publishing of tightly controlled information on various web pages. They do this in efforts to discredit U.S. reports of success and progress in

---


It appears most terrorist organisations are not interested in cyber terrorism. This is because known terrorist organisations like the Al Qaeda are reported to prefer leveraging cyber technologies such as the internet to enable terrorist operations in the physical domain. According to Weimann (2004), there are eight major ways in which terrorists use the Internet. These are psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, information sharing, and planning and coordination.

1. Data Mining and personal data profiling
A large amount of public information is available on the internet, including publicly available maps and building details that could be searched for by a person planning a terror attack. U.S. Secretary of Defence Donald Rumsfeld said in 2003 that an Al Qaeda training manual recovered in Afghanistan tells its readers that "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy." Terrorists can readily gather data about individuals and corporations and even national governments over the internet. Interestingly, these free services are provided by companies such as Google, Yahoo and Microsoft without the need for verification of personal identity. Terrorists have learnt that with little technology and the deployment of search engines, not only is public information accessible to them, it is also possible to trace the subliminal interests of private individuals by tracking the websites they visit and thus reach out to sympathisers and potential terrorists.

2. Recruitment and radicalisation of intending terrorists
Further to the above, terrorist organisations are able to monitor users who browse their websites, capture their profile and information about them and if deemed possibly useful to their cause, are contacted. This grooming process starts from when the user begins to absorb the propaganda on the website, for example the often discussed "charismatic" style of delivery that Osama Bin Laden employs on his video messages. Perhaps motivated by this video, the user seeks answers to questions and goes to internet chat-rooms and discussion boards. Possible recruits are spotted by lurking recruiters who through gradual encouragement of discussion of religious issues to gradually including more political discussions. This grooming leads the recruits to become more and more entangled in terrorist related discussions and are led through a maze of private chat-room’s until personal indoctrination occurs which is often through the use of the secure software.

3. Cybercrime is a Source of Funding for Terrorism

---

47 Supra, note 44
50 A good example is Google Maps.
51 Weimann, op cit.
Since money is the lifeline of terrorism, terrorist groups have made full use of the Internet's ability to create funds; whether legitimately or otherwise. The main methods that the terrorists achieve this by are:

(a) Goods selling: merchandise that is directly related to the terrorist organisation, for example, CDs, DVDs and books from the LTTE.
(b) Website and email based appeals: sending emails to sympathizers who registered interest on a group's website, posting messages on newsgroups/forums and their own websites that give directions as to how and where donations can be made.
(c) Deception: using seemingly legitimate charities or businesses that unknown to the donator, directs the funds to terrorist organisations.
(d) Criminal activity: Illegitimate means of gaining funds that terrorist groups are known to use include credit card fraud, online brokering and gambling and identity theft.

In a November 2007 speech given to Penn State Students by Robert S. Mueller, he cites a case where an infamous al-Qaeda sympathizer and supporter based out of the United Kingdom known as “Irhabi 007” stole thousands of credit card numbers through elaborate phishing schemes. He then used the card numbers to purchase over $3 million in equipment needed for terrorist operations. This is a good example of how a small group of people with small budgets and access to the Internet can make an enormous financial impact on terrorist organizations.

4. Disinformation

The use of disinformation by terrorist groups is often used to incite fear, panic and hatred by sending threats, creating psychological attacks through the use of threats of cyber-terrorism and airing videos of brutal executions. One of the earliest examples of this was the kidnapping of a certain Kenneth Bigley in Baghdad in September 2004 alongside two American colleagues. Two days later, a video was released of the three men kneeling in front of the captors’ banner and on the 21st, a video of the killing of the two Americans was released. Eventually, after some videos were shown of Bigley pleading for his life, he was shown beheaded in October of the same year. Disinformation has been used successfully to incite violence by certain militant groups.

Disinformation may also be used to divert attention from an impending attack by releasing details of a hoax attack so that governmental and law enforcement agencies are side-tracked. However, this may not be wholly effective given the nature of current security climates; that is upon receiving information on a potential attack, the security level on all spectrums across a whole country is increased i.e. from black to black special or similar.

5. Communication and Networking

Terrorist groups have over time changed from having a clearly defined hierarchy in the organisations with designated leaders, to having multiple, semi-independent cells with no clear distinct leader in order to allow them to remain hidden. The Internet facilitates communication between cells which allows exchange of information and manuals. It has also helped terrorist groups gain notoriety from other groups such as 'jihadist' sites. The continual pressure from law

---

enforcement has forced many terrorist groups to evolve and become more decentralised, and this structure is perfectly assisted by the internet.

The internet offers a great way for like-minded people located in different places regardless of their motives to interact easily. This is particularly important when the persons involved may be isolated and have to work more clandestinely or surreptitiously. Without the opportunities of meeting in normal places and organising themselves towards their missions, many terrorist groups are alleged to have created virtual communities through chat rooms and websites in order to continue spreading their propaganda, teaching and training. In the words of Tibbetts, “information technology gives terrorist organizations global power and reach without necessarily compromising their invisibility.”

6. Publicity and Propaganda
Terrorist engage in publicity, and propaganda and this is a form of psychological warfare. The possibilities in cyberspace have significantly enhanced the possibilities for terrorists to have more publicity than before the days of wide internet access. All too often we are reminded that terrorism continues to inflict pain and suffering on people all over the world. And hardly does a week go by without the media reporting that some murderous act of terrorism has taken place somewhere on the globe. And most of the times, video clips of these terrorist organisations get to media houses for onward display to the sorrow of rest of the world but to the joy of the terrorists.

7. Planning and Coordination
Terrorists have also learnt to use the internet to keep their decentralised command of leadership in close touch for ease of planning and coordination of terror attacks. It is reported that Al Qaeda operatives relied heavily on the internet in planning and coordinating the September 11 attacks on the United States. To preserve their anonymity, the al Qaeda terrorists used the Internet in public places and sent messages via public e-mail. Some of the September 11 hijackers communicated using free web-based e-mail accounts. Hamas activists in the Middle East, for example, use chat rooms to plan operations and operatives exchange e-mail to coordinate actions across Gaza, the West Bank, Lebanon, and Israel. Instructions in the form of maps, photographs, directions, and technical details of how to use explosives are often disguised by means of steganography, which involves hiding messages inside graphic files.

Legal Responses against Terrorism

56 Weimann, G. op cit
57 Sometimes, however, instructions are delivered concealed in only the simplest of codes. Mohammed Atta’s final message to the other eighteen terrorists who carried out the attacks of 9/11 is reported to have read: “The semester begins in three more weeks. We’ve obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering.” (The reference to the various faculties was apparently the code for the buildings targeted in the attacks.)
Draft Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference

A lot of measures have been put in place to fight terrorism both at national levels and regional levels. Internet-based terrorist actions are not left out either. Presently, there are about 18 universal instruments\(^{58}\) against international terrorism within the framework of the United Nations system relating to specific terrorist activities. Through the General Assembly, member states have been coordinating terrorism efforts while the Security Council has been active through Resolutions and establishing subsidiary bodies.

But a look through the various Conventions and Protocols does not reveal any direct effort made at addressing the illegal deployment of information communication technologies in carrying out terrorist acts until very recently. On the 8\(^{th}\) of September 2006, the United Nations Global Counter-Terrorism Strategy was adopted by member states.\(^{59}\) The strategy, in the form of a resolution and an annexed plan of action is supposed to be a unique global instrument that should enhance national, regional and international efforts to counter terrorism. One of the measures in the Plan of Action was to address the conditions conducive to the spread of terrorism. It is odd that no attention was given to the proliferation of information communication technology much at that time, less addressing the challenges thereby.

However the United Nations began to take more serious steps in this regard in the 2010s. In 2013, the General Assembly adopted resolution 68/243 and requested the Secretary General to establish a Group of Governmental Experts\(^{60}\) comprising of 20 members that would report to the General Assembly in 2015. The Group made four general findings among others:

1. In their use of ICTs, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.
2. Existing obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms.
3. States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.
4. The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour.

In his own foreword to the report, the Secretary General observed the dangers of ICTs being freely used by extremists and criminally minded persons and noted that:

"Few technologies have been as powerful as information and communications technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can only be achieved through international cooperation, and the

\(^{58}\) Fourteen instruments and four amendments.
\(^{60}\) Experts from the following member states participated Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russian Federation, Spain, United Kingdom and United States of America. (Sadly, Nigeria was missing)
The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security. The report concludes that the United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States and developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour.

It may be necessary here to examine some other regional provisions in this regard. The European Convention for the Prevention of Terrorism was signed in Warsaw on May 15, 2005. It states that each member state shall take the necessary measures to ensure that in their legal order the intentional acts, which given their nature and context, may seriously damage a country or an international organisation where committed also with the aim of causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, are considered a crime. Indirectly, cyber terrorism is included under this definition.

Globally, there have been some private initiatives. The International Telecommunication Union launched a Global Cybersecurity Agenda (GCA) on 17 May 2007 alongside partners from governments, industry, regional and international organizations, academic and research institutions. The GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society. It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today’s challenges related to building confidence and security in the use of ICTs.

Within ITU, the GCA complements existing ITU work programmes by facilitating the implementation of the three ITU Sectors’ cybersecurity activities, within a framework of international cooperation. The Global Cybersecurity Agenda has seven main strategic goals, built on five work areas: 1) Legal measures; 2) Technical and procedural measures; 3) Organizational structures; 4) Capacity building; and 5) International cooperation.

The Nigeria Cybercrimes Act 2015.

---

62 Ibid
63 Article 1
65 Global Cybersecurity Agenda (GCA), is available at [www.itu.int/cybersecurity/gca/](http://www.itu.int/cybersecurity/gca/)
Draft Paper Presented at 49th Annual Nigerian Association of Law Teachers (NALT) Conference
After years of efforts and pressure from different sectors of the society, the National Assembly towards the exit of the last administration enacted the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015. The explanatory memorandum to the Act states that the Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act also ensures the protection of critical national information infrastructure and promoted cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programmes, intellectual property and privacy rights.

The Act attempts to preserve the nation’s critical information infrastructure and in doing so firstly mandates the President on the recommendation of the National Security Adviser to designate certain computer systems and networks as critical national information infrastructure and thereupon to prescribe minimum standards, guidelines, rules or procedure in respect of their protection and preservation, the general management thereof, access to, transfer and control of data in any critical national information infrastructure.

The Acts goes further to create certain offences and stipulates penalties thereof. These are offences against critical national information infrastructure, offences of unlawful access to a computer, offences of perpetration of electronic fraud online, offences of system interference, intercepting electronic messages, willful misdirection of electronic messages, computer related forgery, computer related fraud, theft of electronic devices, unauthorized modification of computer systems, hindering the functioning of computer systems, forging of electronic signatures,.

The Act makes a bold move in Section 18 by creating the offence of Cyber Terrorism. The Act states that “any person that accesses or causes to be accessed any computer or computer system or network for the purposes of terrorism commits an offence and is liable on conviction to life imprisonment”. Terse as this statement may appear, it is capable of covering both incidents of terrorism in the cyber environment and also any other attempt to use computers or networks to initiate or promote or carry out real life terrorist operations in the physical world.

The Act also provides for the administration and enforcement of its provisions and places the responsibility for the coordination of all security agencies under the Act on the office of the National Security Adviser and the office is to provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria. The office of the NSA is also to establish and maintain a National Computer Emergency Response Team (CERT) Coordination Centre, responsible for managing cyber incidences in Nigeria. In addition, the office of the NSA is to coordinate Nigeria’s involvement in international cyber security cooperation to ensure the integration of Nigeria into the global frameworks on cyber security.

Conclusion.

66 Section 3
67 Part III of the Act is headed Offences and Penalties comprising Sections 5 – 36.
68 Section 41(1)
69 Section 41(1) (c)
70 Section 41(1) (g)
Cybersecurity is a global problem that has to be addressed globally by all governments jointly as no government can fight cybercrime or secure its cyberspace in isolation. According to a KPMG Forecast,\(^{71}\) experts believe that to fight the borderless and continuously evolving cybercrime, global leaders must collaborate in joint initiatives.

Countering the threat of terrorism is an epic challenge for law enforcement given the uneven playing field in the cyber environment.\(^{72}\) Unlike the terrorist, law enforcement officers must play by the rules set forth in the law and policy designed to preserve the fundamental human rights of law abiding citizens. Sadly, most of the times, terrorists and their accomplices are made aware of law enforcement techniques and strategies due to leaks announced by the media.

Another major challenge has to do with the need to secure a balance of interest between the preservation or protection of individual rights in cyberspace and the urgent need to crack down on terrorist activities wherever they may be found. Applying counter terrorism measures indiscriminately may impose on the people authoritarian governments and agencies with little or no public accountability tools which may lead to violation of privacy, curtailing the free flow of information, restriction on the freedom of expression and overall heavy price in terms of reduced civil liberties.\(^{73}\)

Due to the nature of the internet and the possibilities of secured information processes via information communication technology, identifying and capturing the terrorist in the cyber domain is becoming increasingly difficult. There are in existence a lot of sophisticated and powerful tools which enable them to be anonymous.\(^{74}\) Further, terrorists and cybercriminals generally employ the technique of constantly relocating websites from server to server essentially making it difficult to shut sites down.

It seems from the foregoing that it is clear that no singular nation on earth (no matter how powerful) can stop global terrorism and terrorist operations in cyberspace. But then due to the territorial nature of criminal law, each nation should have definite laws and cyber security policies to secure its own cyberspace from criminals who are constantly looking for cyber-havens. Just as nations and regions within the permissible limit of international law are forging relationships, this should be followed up with relevant treaties towards jointly securing cyberspace as a whole.

Quite a number of the powerful nations on earth are selfish and territorial conscious. There is no consensus among these nations about the best method to secure the global cyberspace. This is one reason why it has been pointed out that a Cyberspace treaty is at best a pipe dream. It seems the ideological difference among nations is a major hindrance. However, the United Nations Office on


\(^{72}\) Chargualaf, op cit.

\(^{73}\) Weimann, op cit.

\(^{74}\) Wilson, C. “Emerging Terrorist Capabilities for Cyber Conflict Against the U.S. Homeland.” (Congressional Research Service of the Library of Congress, 1 Nov 2005), 6
There is the need for constant updating of the knowledge base of law enforcement dealing with cyber crime and terrorist activities. A report released as far back as 2003 by the United States Drug Enforcement Agency found that 14 of the 36 groups found on the US State Department list of foreign terrorist are involved in drug trafficking. This led the DEA to suggest that the war on terror and the war on drugs should be linked. The challenge here is that it is more difficult to predict terrorist behaviour that falls outside established patterns.

However, despite all the above challenges, the war on terror will continue to shift to every battleground that terrorists shift to. Therefore, we must become better informed about the uses to which terrorists put the Internet and better able to monitor their activities. As noted by Weimann, journalists, scholars, policymakers, and even security agencies have tended to focus on the exaggerated threat of cyber terrorism and paid insufficient attention to the more routine uses made of the Internet. Those uses are numerous and, from the terrorists’ perspective, invaluable. Hence, it is imperative that security agencies continue to improve their ability to study and monitor terrorist activities on the Internet and explore measures to limit the usability of this medium by modern terrorists.