INFORMATION TECHNOLOGY, TERRORISM FINANCING AND FINANCIAL INSTITUTION'S ROLE IN COMBATING TERRORISM[1]*

Abstract:

In these contemporary times, modern means of information technology that includes the internet and cyberspace are not only employed for positive commercial and political gains but also for criminal strategies that include advancement of terrorism. Counter terrorism frameworks must also engage similar tools if it must remain effective in the contemporary fight against this hydra headed phenomenon. This article examines the counter terrorism landscape and its intersect with modern communication technology innovations. Reflecting the new threat and challenge that modern means of terrorism pose to the counter terrorism community, this article argues more prominently that effective and successful counter terrorism seeking to address contemporary methods of terrorist recruiting, financing and warfare, require a collaborative and multilateral cooperation amongst nations and stakeholders. In addition, a counter terrorism information technology bias is critical to successful counter terrorism efforts.

Keywords: Terrorism, Communication Technology, Cyberspace, Internet, United Nations, Terrorism financing.

1. Introduction

Modern forms of terrorism are often carried out reflecting intense sophistication in planning, organizing, coordination and execution. More often than not, the scale in fatalities in injuries and loss of life it brings to the civilian population is unimaginable. Post terrorism investigations have shown that beyond the physical planning of many terrorism occurrences, there is a virtual space provided by modern means of technology which aid the execution of terrorists' threats and activities. It is not unsurprising that the international community has begun to focus its energy and resources to counter terrorism legal structures and strategies that address the use of modern communication technology for terrorism operations. This work is another effort in the direction of the same energy and seeks to showcase that effective counter terrorism in the contemporary era must as matter of course checkmate the misuse of internet and other forms of modern media which are being employed for terrorism related activities. Related to these modern media technologies abuse is the use of the same means which facilitates terrorism financing and funding by wire transfer to and from masquerade charity houses. This article argues that a robust synergy is needed in terms of legislative structures and institutional control measures amongst States and stakeholders if we are to pace up with the same of level of sophistication associated with technology based terrorism maneuvers. In consequence, this paper first examines the architecture of modern communication technology under the shadow of counter terrorism landscape, while drawing some important distinctions between cyberspace, cybercrime and cyber terrorism. Further it underscores the emerging legislative efforts from within the UN as an international body as well as some institutional frameworks for the purpose of policing terrorism that is technology savvy. In the final section, the paper undertakes a detailed study of counter terrorism approaches to combatting the financing of terror in the present era of new technology adopted by modern banking practices.

2. Modern Communication Technology and Counter-Terrorism Landscape

When governments like Nigeria or Paris are challenged by the menace of terrorism on astronomical scale with considerable frequency in occurrence, one of the most pressing policy issues becomes the adequacy of allocation of resources for effective and optimal counter terror outcomes. In many cases involving recent terror incidence in Europe and Africa, it has been shown that when terrorists observe an increase in a particular counter terrorism program, they tend to switch tactics, devising new tactics that are less affected by the government efforts. For instance, when the hysteria was so much on aviation industry in the post 9/11 period, resources was allocated to airport and airline security across the globe, but then terrorists made a shift by attacking inbound transportation

[1]*By **Emeka C. ADIBE Ph.D,** Lecturer, Faculty of Law, University of Nigeria, Enugu Campus;
***Ndubuisi NWAFOR Ph.D,** Lecturer, Faculty of Law, University of Nigeria, Enugu Campus; and
* **Chibuike AMAUCHEAZI**, Lecturer, Faculty of Law, University of Nigeria, Enugu Campus.

systems, tourist sites, international centers, and embassies and other enemy interests abroad. They also began to utilise resources available to globalisation, which is the upscale communication technology by recruiting home grown terrorists via the internet encouraging them to carry out lone wolf attacks. At the same time, the electronic mode of banking facilitated by modern technology was also exploited by organisations and individuals for the purpose of financing terrorism. It is obvious therefore that any legal system that fails to accord a primal role to information technology for effective and comprehensive counter terrorism measures will be sidestepping a very significant aspect of terrorism in the present 21st century. Granted that information technology (internet) is a welcome positive revolution, it has affected every aspect of life, for some of them, in a negative way. For instance, it has facilitated the spread and ease with which terrorism is financed and terrorists recruited. African and Nigeria in circumspect have also not been spared these negative impacts of information technology as regards the financing of terrorism, spread of its agenda and the publicity that it feeds on in order to achieve its desired effect. An enormous amount of threats coming from terrorist organisation happen in the cyber space. Also the financing of terror by organisations masquerading as charities also happen more predominantly through bank transactions which also employ the benefits of instant transfer of funds made possible by present day information technology.

The fallout of this trend is that counter terrorism efforts must also migrate its efforts in a more proactive and adaptive way into policing the cyberspace[2] in order to counteract the challenges posed by the complex and evolving menace of financing and spread of terrorism through the medium provided by modern information technology paraphernalia.

3. Cyberspace, Cybercrimes and Cyber-Terrorism

Apart from using the internet and modern means of information technology to facilitate terrorism, it is apt to make some necessary connection between cyber space, cybercrimes and cyber terrorism. Crimes committed using the cyberspace mechanism and outfits are technically called cybercrime. Activities carried out over the internet become a cybercrime when they involve activities which are considered illegal, criminal and are prohibited under the law regulating such activities in the cyberspace and involve abuse and misuse of computer and information data. Alobo describes ‘cybercrime as criminal activities committed through the use of electronic media.’[3]However, when illicit activities are carried out or committed in the cyberspace with the intention to disrupt the free flow of information, distort cyberspace networks and the data stored therein, and for the purpose of causing harm or threat of serious harm in order to achieve a political purpose, it is called cyber terrorism. Cyber terrorism is therefore a form of cybercrime. In this instance, the target is the cyber space not the physical space or individuals. This is dissimilar to employing the gains of internet technology and utilising them as an accessory to finance and facilitate the spread of terrorism. While the latter is not itself a criminal act, its end result is criminal, the former is intractably criminal hence termed cyber terrorism. The common denominator in these two themes is that internet has been used directly as viable tool in the case of cyber terrorism and indirectly in the case of spread and aiding terrorism to commit terrorism crimes (a form of cybercrime) respectively.

Cyber terrorism which is convergence of terrorism and cyberspace constitutes a major threat to critical national infrastructures such as the security systems, embassy networks, email servers, aviation control systems with deleterious consequences which speaks to the fact that tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb. Cyber terrorism is an attractive option for modern terrorists,[4] who value its anonymity,

[2] Cyber space refers to the electronic medium of computer networks in which online communications takes place. See Joshua. E. Alobo, *Terrorism, Kidnapping and Cybercrime in Nigeria* (Abuja: Diamond real Resources Consult, 2013), 159.

[3] J. E. Alobo, *Terrorism, Kidnapping and Cybercrime in Nigeria* (Diamond Real Resources Consult Abuja, 2013)167.

[4] The Appeal of Cyber terrorism for Terrorists: Cyber terrorism is an attractive option for modern terrorists for several reasons. • First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection. • Second, cyber terrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—”screen names”—or log on to a website as an unidentified “guest user,” making it very hard for security agencies and police forces to track down the terrorists’ real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

its potential to inflict massive damage, its psychological impact, and its media appeal. Unfortunately, invasive inroads in the military campaign on terror are likely to make terrorists turn increasingly to unconventional weapons, such as cyber terrorism. And as a new more computer-savvy generation of terrorists comes of age, the danger seems set to increase.

Although cyber terrorism does not entail a direct threat of violence, its psychological impact on anxious societies can be as powerful as the effect of terrorist bombs. Combating cyber terrorism must therefore be given priority if a comprehensive counter terrorism model is to be contemplated. In this context, Gabriel Weimann[5] argues that the next generation of terrorists is now growing up in a digital world, one in which hacking tools are sure to become more powerful, simpler to use, and easier to access. The terrorist of the future will win the wars without firing a shot - just by destroying infrastructure that significantly relies on information technology. The fast growth of the Internet users and internet dependence dramatically increased the security risks, unless there are appropriate security measures to help prevention. Cyber terrorism may also become more attractive as the real and virtual worlds become more closely coupled. For instance, a terrorist group might simultaneously explode a bomb at a train station and launch a cyber-attack on the communications infrastructure, thus magnifying the impact of the event. Unless these systems are carefully secured, conducting an online operation that physically harms someone may be as easy tomorrow as pulling a trigger. Realizing the potential danger of cyber terrorism after the 9/11 attacks, President Bush created the Office of Cyberspace Security in the White House and appointed his former counterterrorism coordinator, Richard Clarke, to head it.

4. Legislative Frameworks for Countering Communication Technology Driven Terrorism

Cyber terrorism and other forms of terrorism facilitated by the cyberspace constitute a new threat and challenge in this era of terrorism. In recognition of this, the international community has turned some of its focus to the development of principles, necessary for the enforcement of international obligations for the suppression of financing of terror as well as to the issues related to countering the use of the internet for terrorist purposes. These efforts speak to the fact that the effective counter terrorism measures must contemplate a crusade against financial support of terrorism which cannot be won inside the boundaries of individual countries working alone, a situation made possible by the fluidity of the internet with its digital ability to blur differences in time and geographical location embedded in e-commerce content of banking relations and transactions. (The world has become a global village via the internet and business activities are conducted at the speed of light through the instrumentality of computer networks.)[6]

The new information technologies (IT) and the Internet are more often used by terrorist organizations in conducting their plans to raise funds, distribute their propaganda and secure communications.[7] The convicted terrorist, Ramzi Yousef, the main planner of the attack on the World Trade Centre in New York stored detailed plans in encrypted

• Third, the variety and number of targets are enormous. The cyber terrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency services, are vulnerable to a cyber-terrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses. • Fourth, cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyber terrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers. • Fifth, as the I LOVE YOU virus showed, cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want. See Gabriel Weimann, United institute of Peace, Special Report, 119, Dec. 2004 available at: <https://www.usip.org/sites/default/files/sr119.pdf> accessed 03/12/16

[5] Gabriel Weimann, United institute of Peace, Special Report, 119, Dec. 2004.<https://www.usip.org/sites/default/files/sr119.pdf>accessed 03/12/16

[6] Alobo, (n.3) 159.

[7] Ikenga K.E. Oraegbunam & Kenneth U. Eze, 'The Internet and its Facility for Criminality: Some Unique Difficulties for Investigation and Prosecution',*Nnamdi Azikiwe University Journal of International Law and Jurisprudence,* Vol. 5, 2014, pp.12-26. Available at http://www.ajol.info/index.php/naujilj/article/view/136271.

files in his laptop computer for aircraft destruction in the United States. Terrorist organizations also use the Internet to ‘reach out’ to their audience, without need to use other media such as radio, television or holding various press conferences. The internet also helps individuals acting as terrorists (lone wolf) to engage in terrorist activities. In 1999, a terrorist-David Copeland killed 3 people and injured 139 in London. He did this with the help of bombs placed in three different locations. At his trial it was discovered that he used Terrorists Manual (Terrorist Handbook - Forest, 2005) and How to Make a Bomb (How to Make Bombs -2004), which he had downloaded from the Internet.[8]

The Counter Terrorism Committee established by Security Council is the body saddled with the duty to monitor cyber security and it appears tremendously in the UN Global counter terrorism strategy. The goal is not only to counter terrorism in all its forms and manifestations on the Internet, but also with more active approach to use the Internet as a tool for countering the spread of terrorism. The collaborative approach to countering the use of internet for purposes of facilitating terrorism would oblige countries to closely monitor web pages of the terrorist and extremist organizations and to exchange information with other governments in the international scene and other relevant forums. It also demands a more active and pro-active participation of civil society institutions and the private sector in preventing and countering the use of the internet for terrorist purposes. In the UN system, the International Telecommunication Union (ITU) has the highest responsibility for the practical aspects and applications of the international cyber security. The purpose of the organization is to develop confidence in the use of cyberspace through enhanced online security. Bogdanoski and Petreski[9] identify some of notable examples of cyber terrorism which cut across cyber threats to Sri Lanka, India, China, Romania and Palestine.[10] Apart from the use of internet for offensive operations, terrorists can effectively use the cyberspace for secure communications. Immediate concerns also include the use of cyberspace by terrorists for covert communications, for wire transfers, terrorist instructions hidden online and web encryption messages by terror groups.

Many governments in an effort to check cyber terrorism and other forms of terrorism facilitated by the use of cyberspace has set limits by way of legislative frameworks for monitoring telephone calls, surveillance and monitoring e-mails and bank accounts and even introduced legislations permitting Security Intelligence Agencies to intercept electronic mail of persons suspected of terrorist activities with the aim of an attack directed against the preparation and planning of terrorist acts. In some situations, the law even allows the terrorist property to be frozen or taken away. Legislative frameworks both at the international and domestic sphere must work from two prongs of directing efforts first at countering the use of internet for terrorist purpose and secondly suppressing the financing of terror. In the first case, one has to note that terrorists have employed the use of internet by disseminating their data and information through the use of websites hosted by them. The legislative arrangement has to be structured in such a way that the identity challenges prevalent in cyberspace architecture are surmounted for the purposes of leveraging

[8] Mitko Bogdanoski & Drage Petreski, Cyber Terrorism– Global Security Threat [2013] *International Scientific Defence, Security And Peace Journal.* July 2013 .<https://www.researchgate.net/publication/252195165_CYBER_TERRORISM-_GLOBAL_SECURITY_THREAT> accessed 03/12/16.

[9] Ibid 6.

[10] In 1988, a terrorist guerrilla organization, within two weeks, flood embassies of Sri Lanka with 800 email-s a day. The message which was appearing was “We are the Internet Black Tigers and we are doing this to disrupt your communications.” Department of Intelligence characterizes the attack as the first known terrorist attack on government computer systems. Internet saboteurs in 1998 attacked Web site of the Indian Bhabha Atomic Research Centre and stole e-mails from the same center. The three anonymous saboteurs through online interview claimed that they protest against recent nuclear explosions in India. In July 1997, the leader of the Chinese hacker group claimed that temporarily disallowed Chinese satellite and announced that hackers set up a new global organization to protest and prevent investment by Western countries in China. Romanian hackers on one occasion managed to intrude into the computer systems controlling the life support systems at an Antartic research station, endangering the 58 scientists involved. Fortunately, their activity is stopped before any accident occurred. During the Kosovo conflict, Belgrade hackers conducted a denial of service attack (DoS) on the NATO servers. They “flooded” NATO servers with ICMP Ping. During the Palestinian-Israeli cyber war in 2000 similar attack has been used. Pro-Palestinian hackers used DoS tools to attack Israel’s ISP (Internet Service Provider), Netvision. Although the attack was initially successful, Netvision managed to resist subsequent attacks by increasing its safety messages, typically used for diagnostic or control purposes or generated in response to errors in IP operations.

robust cyberspace law enforcement for counter terrorism ends. No longer will people hide under the anonymous character of online activities as they can be traced using the means of numeric identification via internet protocol address which invariably lead to the real geographical location of the criminal or terrorist. Where it is impossible to achieve this kind of attribution to online activities, counter terrorism in this age of technology stands to be frustrated without achieving great results. Hence the Counter Terrorism Implementation Task Force (CTITF) recognises this fact when it concludes that:

> Without attribution, it was impossible to determine if a particular cyber-attack or intrusion was the work of lone teenage hacker testing his skills, an international organised crime group seeking to commit a major financial fraud, a terrorist entity launching a denial of service attack against a vital critical infrastructure or a nation state engaging in cyber warfare.[11]

The Counter Terrorism Implementation Task Force (CTITF) therefore makes a proposal for robust identity systems for all internet regulation systems for both at the international level and domestic level, while respecting the boundaries of human rights and data privacy. Again policy and legal measures that enhance the ability of authorities to respond to the challenges posed by terrorist anonymity on the internet must be adopted. Such measures would include requiring identification from those using cybercafé, purchasing SIM card for mobile technology as well as mandatory requirement for data retention by communication or internet providers. The robust policing of the internet would also significantly address the use of internet as a tool for propaganda, radicalisation and recruitment. While some of the content in the websites would assist gaining insights into their activities for counter terrorist initiatives; some efforts where and when necessary should be made to pull down their sites, block access to the content of those sites through national firewall systems and content filtering systems. Recognising the prevalent difficulty of blocking terrorists' content in cyberspace, it has been proposed in some quarters[12] for purposes of counter terrorism, to allow terrorist websites to remain operational in order to monitor the online activities for intelligence and law enforcement purposes and as well create opportunity to influence their discussions in online forums. What is considered expedient in this connection is endeavoring to maintain a balance between blocking the website of terrorist cells and allowing them to operate for counter terrorism intelligence and initiatives.

5. Institutional Frameworks, Counter- Terrorism and Communication Technology

At the institutional level, Interpol has launched a unit in 2009 known as 'Monitoring Assessment and Partners' (MAP). The goal of MAP is to monitor terrorist websites and disseminate any valuable information uncovered to national police forces around the world. Following the efforts of the Interpol, some governments have developed some similar initiatives for policing terrorist's activities on the cyberspace. Germany established a Joint Internet Centre- a multi-agency effort to gather information on terrorist activities in cyberspace; also the European Union Police Office (Europol), established a secure online portal known as 'check the web' which allows police officials of the twenty seven EU members to share data uncovered online regarding terrorists' activities. Jurisdictions like Nigeria infested with incessant incidences of terrorism facilitated by the use of contemporary forms of communication need to develop such initiatives if any counter terror efforts would come to any measurable success.

Nigeria enacted the *Nigeria Cyber Crime Act 2015*. Its overarching objective is to secure and regulate the Nigeria cyberspace and ensure that it squares with international standards for the purposes of combating new forms of criminal activities prevalent on the cyberspace following recent communication methods. In addition to its objective of providing an effective and unified legal regulatory and institutional framework for the prohibition, prevention and detection, prosecution and punishment of cybercrimes in Nigeria, it seeks to promote cyber security, protect electronic communications, data networks and programs.

[11] CTITF Working group on Countering the Use of Internet for Terrorists Purposes, Technical Issues<http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pd> accessed on 19/03/16.

[12] Ibid.

In section 18 of the Act, cyber terrorism was created as an offence. Thereat, it provides that any person who accesses or causes to be accessed any computer system for the purpose of terrorism as defined under Terrorism Prevention Act (*TPA) 2011* (as amended), is liable to life imprisonment upon conviction. Any adequate construction of cybercrime in Nigeria must be rooted in the definition of terrorism as enshrined in TPA (Amendment Act), 2013. It is one thing to establish the legal framework for such crime as cyber terrorism, it is yet another to set up the necessary institutional frameworks to monitor cybercrime for purposes of counter terrorism. While it may be acknowledged that regulatory scheme for cyber space may have improved from what it used to be prior to enactment of Cyber Crime Act, 2015, the institutional capabilities remain inadequate to the task of suppressing cyber terror or in fact cybercrimes in general. The setting up of the Computer Emergency Response Team (CERT) under the Cyber Crime Act 2015 as well as the Communication Commission under the Nigerian Communications Act 2013 is a welcome development whose duties are to monitor the cyber space for intrusions and disruptions capable of hindering the proper functioning of the system networks. These agencies are empowered to respond to cyber threats that may affect the country's communication system including terrorism threats on the cyberspace. Interception is the key to effective counter terrorism. The strengthening of these agencies to achieve their optimal value will remarkably work success in the area of policing the cyberspace for purposes of terrorism prevention in Nigeria.

6. Combatting Terrorism Financing

Following popular business trend, people and organisations including terrorists have turned to e-commerce as a means of raising funds for their activities. Mathew Levitt observes that, 'Investigation into al Qaeda sleeper cells in Europe in the wake of September 11 revealed the widespread use of legitimate businesses and employment by al Qaida operatives to derive income to support both themselves and their activities.'[13] Similarly, legitimate employment offers terrorists cover, livelihood and sometimes useful international contacts. Donations to terrorist causes are often made through electronic transfers and credit cards using various charitable organisations through which they solicit funds promising to use the money for philanthropic purposes. Other techniques are also used to raise funds online for their extremist activities. In addition to this, like other legitimate organisations, terrorist organizations are also using social networking applications as the latest method for raising funds for their illicit activities. The CTITF report succinctly confirms this fact in these words:

> There is substantial evidence that terrorist organisation are using the proceeds from traditional cybercrime, such as online credit card fraud, identity theft and telecommunications fraud to fund their operations. Even in the dawn of the internet revolution, terrorists were exploiting technology as a means of fundraising.[14]

In the light of this development, emerging technologies have facilitated the propensity of terrorists to hide and move money around the globe for the purposes of their operations. In another research conducted by Mark Cantor, it spells out that, 'The sources and methods of funding terrorism networks have grown widely diversified. Among the sources are donations to charities, use of shell companies and otherwise legitimate business and narcotics trafficking.'[15] The use of charitable organisation for financing terror presents a sensitive challenge, hence effort must be made to discern between legitimate organisations and those hijacked by terrorists to divert funds and support terrorism. Some government like the United States of America and Canada[16] have hitherto in the past issued series of financial blocking orders targeting terrorist front companies or organisations and even raiding their offices for clues for terrorism support and financing. The complicated and trans-boundary nature of modern vehicles for terrorist financing as well as the matrix of international, logistical, financial and coordinated operational mode of terrorist activity make it very difficult to counter through unilateral action of one state. What it means is that states

[13] M. A. Levitt, The Political Economy of Middle East Terrorism, [2002] *Middle East Review of International Affairs*, December, Vol. 6, No. 4, 51.

[14] Ibid.

[15] Mark Cantor, *Effective Enforcement of International Obligations to Suppress the Financing of Terror*, The American Society of International Law Task Force on Terrorism, ASIL Task Force Papers, Sept 2002.

[16] M. A. Levitt, (n.13) 58

must join efforts in the collective creation of measures to track and counter extremist activities fueled by funds meant to encourage such activities. There is need to establish a financial coalition that is intended to rehearse the regulation of financial institutions to levels that will effectively enable the implementation of rules for purposes of counter terrorism at the international level.

In 1999, the United Nations came out with an International Convention for the Suppression and Financing of Terror.[17] The Convention entered into force on 10th April 2002. The Convention strives to cut off what can be regarded as the lifeblood of terrorism of all types, i.e. the provision of material, chiefly financial resources to terrorists. The objective of the Convention is to enhance international cooperation among States in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators. Any person commits an offence within the meaning of the Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or with the knowledge that they are to be used, in full or in part, to carry out any of the offences described in the treaties listed in the annex[18] to the Convention, or an act intended to cause death or serious bodily injury to any person not actively involved in armed conflict in order to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act.

The Convention in addition to criminalization of terror financing, requires each Party to take appropriate measures, in accordance with its domestic legal principles, for the detection and freezing, seizure or forfeiture of any funds used or allocated for the purposes of committing the offences described. The Convention may be criticized for its lack of enforcement measures being a document initiated from the General Assembly and is dependent on the assent of state parties. The Convention though has a moral bite but is lacking in adequate sanctions and enforcement machinery provisions. The Security Council took over the translation of these obligations into effective administrative measures by the adoption of the resolutions that speak to terror financing. Acting under chapter VII of the United Nations Charter, the UN Security Council adopted a number of strong enactments focusing on the financial aspects of terrorism which are binding on member states pursuant to Article 25[19] and Article 48(1)[20] of the Charter. One of the first of such resolution on suppressing terror financing was the Resolution 1373 of September 28, 2001, enacted just a couple of weeks after 9/11 incident. Other similar resolutions of the Security Council which followed include Res. 1377 (12 Nov. 2001), Res. 1390 (28 Jan. 2002). These latter resolutions oblige states to deny financial support and safe haven to terrorists and freeze assets and economic resources of named terrorists and organisations.

Though a general counter terrorism resolution emanating from the Security Council, in the operative part, Res. 1373 did commence its first article[21] with a provision relating to suppressing the financing of terror while obligating states

[17] International Convention for the Suppression of financing of Terror, Adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999.<http://www.un.org/law/cod/finterr.htm> accessed 7/12/16

[18] Annex: Some of these treaties include among others the following: Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation done at Montreal on 23 September 1971; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973; International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988 and International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

[19] The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.

[20] The action required to carry out the decisions of the Security Council for the maintenance of international peace and security shall be taken by all the Members of the United Nations or by some of them, as the Security Council may determine.

[21] Decides that all States shall: (a) Prevent and suppress the financing of terrorist acts; (b) Criminalize the willful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds

to deny safe heavens to those who finance or support terrorist act and further called on states to become parties to the Conventions and Protocols relating to terrorism. This is a bold and remarkable step because no act of terrorism can prosper without attachment to fiscal planning, logistics and support needed by the foot soldier to execute their violent activities. The logic is that when terrorists are starved of funds with which to obtain lethal materials used for their terrorists activities, 'their power to operate against humanity is greatly restrained thereby rendering their nefarious designs inoperative.'[22] In the context of this kind of activities, money laundering regulations in many jurisdictions are subsisting not only to check corruption or other anti- fiscal policies and but also to ensure that huge sums of money do not go into the wrong hands which will potentially be used for terrorism related activities.

Okeke recommends that legal templates be adopted as tool for suffocating the financial tube that waters the illegality of all acts of terrorism. Thus he insists that 'using lawfare as weapon to control the disbursement of fund in order to check free access of fund by terrorists' organisations is part of lawfare.'[23] As already noted, Res. 1373 establishes a Counter Terrorism Implementation Committee (CTIF) to supervise the implementations of these requirement enunciated in most counter terrorism resolutions. As part of the mandate of CTIF, it seeks to identify with the school of thought who believes that targeting a wide array of groups and organisation funding and transferring terrorist funds is critical to counter terrorism but must be conducted as part of a well- coordinated international effort.[24]In the wake of incessant violent terrorist attacks that appear unstoppable, the international community with the cooperation of powerful states and mutual cooperation of each other must develop joint measures to make the global economy less hospitable for terrorist financing, such measures like freezing the assets and the business interests of powerful individuals fingered as culprits wherever they are located in the global economy.

In Nigeria, the Money Laundering Act and the Terrorism Prevention Act as well as the Economic and Financial Crime Act (2004) criminalise all forms of terrorism financing; however, the institutional capabilities for the task of suppressing terror remain inadequate. At the same time, the establishment of the Nigeria Financial Intelligence Unit (NFIU), (an operations unit of the EFCC), set up under the EFCC Act 2004 and Money Laundering Act (2004) is a step in the right direction. This unit is the Nigeria Arm of the Global Financial Intelligence Units (FIU). Its major objective is to bring Nigeria in compliance with combating of money laundering and financing of terror. This agency requires all financial institutions and designated non-financial institutions under the law, to furnish the NFIU with details of their financial transactions. However, much work is needed to be done at the national and at the international level to effectively counter all financing of terror related activities. States must be willing to embrace this dramatic change to financial disclosure and transparency of their banking practices with an attendant penalty for non-committal and non-implementing states by way of isolating them at the international financial centres and businesses.

Cantor recommends for example that financial institutions from non- implementing states could be denied the right to maintain permanent establishments and corresponding bank accounts in money centers like New York City, London, Toronto, and Paris…Tokyo.[25]While it is agreeable that stemming the flow of terrorist financing will not

should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts; (c) Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities; (d) Prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons.

[22] G. N Okeke 'The United Nations Security Council Resolution 1373: An Appraisal of Lawfare in the Fight Against Terrorism' (June 2014), *Journal of Law and Conflict Resolution* Vol.6(3), 43

[23] Ibid.

[24]Levitt (n.13) 59.

[25] M. Cantor, (n.15).

stamp out terrorism, tackling it represents a critical and effective tool both in reacting to terrorists' attacks and engaging in preemptive disruptions efforts in order to prevent future attacks. Cracking down on terrorist financing denies terrorists the means to travel, communicate, procure equipment and conduct their violent operations.

Above all, effective and successful counter terrorism financing require as of essence multilateral cooperation amongst nations. This cooperation must come in the form of capacity building for developing nations, technical assistance to areas fret with high tide of terror financing operations and sharing of data base by banking and law enforcement agencies of stakeholder countries. To monitor the progress achieved by nations, benchmarks ought to be developed to measure progress with compliance with financial services regulatory and acceptable standards. Nations must therefore develop a rigid system to thwart all forms of terror financing by strict compliance to state regulations that draws from international legal commitments.

7. Conclusion

Terrorism is hydra headed and can be carried out in ways and manner that are often not contemplated or expected. While perpetrators continually contrive ways to effectively carry out their unwholesome operations bringing untold hardship to civilian population and targets, states must not fold their hands and feign helpless and at the mercy of those criminals that are bent on destroying the contemporary democratic values of our modern society, nay liberty. Modern communication technology paraphernalia no doubt has not only made recruiting of terrorists easier; its planning beginning with transmission of fund through modern banking system using the internet to its execution on soft targets has also been made less difficult .In the same way, countering terrorism must also tailor its operations using the same communication media to prevent, counter, pre-empt and apprehend the perpetrators. This essay has insisted that the trans-boundary nature of terrorism and the sophistication that goes into its planning must be met with efficient cooperation of states ready to follow suit with regulations modelled with international legal instruments that target an unrestrained use of internet and other means of communication for terrorist purposes.