Combating Terrorism with Cybersecurity: The Nigerian Perspective

Article · December 2013

DOI: 10.13189/wjcat.2013.010401

4 authors, including:

Oluwafemi Osho
Federal University of Technology Minna
39 PUBLICATIONS **247** CITATIONS

SEE PROFILE

Adeyinka ADESUYI Falaye
Federal University of Technology Minna
10 PUBLICATIONS **55** CITATIONS

SEE PROFILE

Shafi'i Muhammad Abdulhamid
Federal University of Technology Minna
110 PUBLICATIONS **1,503** CITATIONS

SEE PROFILE

World Journal of Computer Application and Technology 1(4): 103-109, 2013 http://www.hrpub.org
DOI: 10.13189/wjcat.2013.010401

Combating Terrorism with Cybersecurity: The Nigerian Perspective

Osho Oluwafemi[1,*], Falaye Adeyinka Adesuyi[2], Shafi'i M. Abdulhamid[1]

[1]Department of Cyber Security Science, Federal University of Technology, Minna, Niger state, Nigeria
[2]Department of Mathematics/Statistics, Federal University of Technology, Minna, Niger state, Nigeria
*Corresponding Author: femi.osho@futminna.edu.ng

Abstract Recently, terrorism has become one of the biggest threats to the survival of mankind on the planet. Nigeria has had her own share of the effects of this menace. It is evidently a challenge to national security, a sure enemy to national development. No doubt, Information and Communication Technology (ICT) has pervaded every facet of human endeavour, and terrorist groups too are taking advantage of its potentials to recruit, propagate their propaganda, train its members, communicate and conspire, and even to raise money. In this paper, we sought to highlight cyber tools and techniques used by terrorists in Nigeria in their activities, assess the government's response so far and capacity in tackling terrorism, and proffer recommendations that can help mitigate the menace. It was found out that the cyberspace could fast become the biggest promoter of terrorism in Nigeria, and unfortunately, the government does not possess the necessary cyber-capabilities to tackle this in the country. To forestall this, we highlight the need to view the security of the country's cyberspace as the trigger point in developing effective anti- and counter-terrorism strategies, and consequently, put necessary cybersecurity measures in place to this effect.

Keywords Nigeria, Terrorism, Terrorist, Cyberspace, Cybersecurity, ICT, Cyberterrorism, Bill

1. Introduction

Nigeria stands as one of the most diversified ethnically and religiously. The parts that constitute this heterogeneous entity unfortunately are spatially asymmetrical. While some cultures form majority, others can only lay claim to a meager portion on the national space, either in terms of land mass or population.

Consequent upon this diversity, it is not uncommon to find some people, because of their ethnicity, religion or political standing, feeling oppressed, marginalized, persecuted, or exploited; they feel frustrated with their position in the society. And therefore, to express their frustration, they sometimes resort to unlawful use of terror as their form of persuasion.

Terrorism is fast becoming a major constituent of our society today. Terrorist groups are getting more organized and coordinated by the day. They exist, in most cases, with identifiable chain of command or conspiratorial cell structure [1].

The use of ICT as a necessary tool for managing our daily lives is no more debatable. Indeed it has become one of the daily necessities of life. There is hardly any enterprise today that does not utilize this ubiquitous means. In Nigeria, there has been an upward surge in the use of the cyberspace: an average Nigerian uses a mobile phone, while internet penetration is steadily growing. From 2000 to 2012, the country has experienced increase in mobile users (shown in figure 1) from a mere 30,000 (0.02 subscriber per 100 inhabitants) to 112,777785 (67.68 subscribers per 100 inhabitants), and an increase in internet subscription from 0.06 to 32.88 subscriber per 100 inhabitants (represented in figure 2) [2]. Unfortunately, this has led to more abuse of the same cyberspace. Presently, Nigeria ranks among the worst countries when it comes to abuse of ICT [3]. Criminals, terrorists, and other undesired agents of the society use it as aids to perpetrate their unlawful acts.

Terrorism has long ago been recorded in Nigeria. For instance, the Oke-Ogun uprising in 1921 [4], and those carried out by Niger Delta Volunteer Force in 1965 [5] readily come into mind. However, there had never been any record of the use of the cyberspace as means for perpetration. Most of the literatures on terrorism in country only focused on the socioeconomic aspects, for example, in [6,7,8]. This partly could explain why their recommendations were non-IT in nature.

While the deregulation of the telecommunication sector, by law, took place in 1992, it was not until 2000 that Nigeria, via the GSM revolution, began to experience increase in digital inclusion. Hence, it can be assumed that substantial exploitation of the cyberspace to aid terrorism would have commenced around this time. Therefore, considering the rate of cyber-utilization in virtually all sectors in the country, the current need to consider terrorism from this context cannot

be overemphasized.

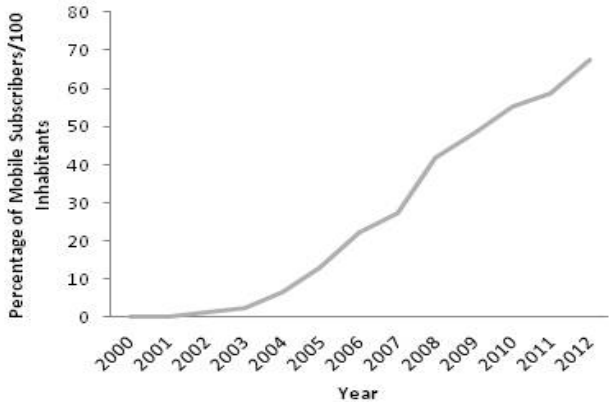

Figure 1. Percentage of mobile subscribers from 2000 to 2012

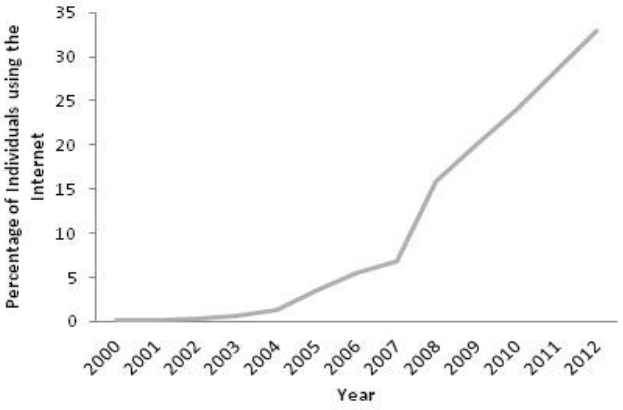

Figure 2. Percentage of internet subscribers from 2000 to 2012

This paper focuses primarily not on attacks on information and communication systems – commonly referred to cyberterrorism – but on the fact that the Nigerian cyberspace is abused, through the improper use of information and communication systems as aids to perpetrate traditional terrorism, and therefore, there is need to secure it. Basically, we seek to highlight cyber tools and techniques used by terrorists in Nigeria in their activities, assess the government's response so far and capacity in tackling terrorism, and proffer recommendations that can help mitigate the menace.

2. Literature Review

2.1. What Constitute Cyberspace

The term cybersecurity is used to "summarize various activities such as 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 organization and user's assets" [9]. Some of these activities include internet filtering, which implies filtering online contents to determine the level of accessibility to be allowed, and can be used to deny access to unwanted websites [10]; wiretapping, that is, intercepting communications over a network [11]; call logging, which means, logging of user's call for the purpose of monitoring and analysis; to mention but few.

Termed the fifth common domain – after land, sea, air and outer space [12], cybersecurity involves, but is not limited to, all machineries employable for the protection of the cyberspace, including protection against the abuse of the cyberspace.

2.2. Traditional Terrorism and Cyberterrorism

Both terms have been used interchangeably, and assumed different meanings. Computer security professionals, law enforcement agencies, lawmakers, all have professionalized meanings. Heickero [13] defined cyberterrorism as relating to activities against critical information infrastructure, while traditional terrorism connotes threat of or outright violence, geared towards achieving an aim. Zalman [14] extrapolated the definition of cyberterrorism to also include that associated with traditional terrorism. Most definitions tend to agree more with Heickero's. One common denominator in all considerations is the capacity of any type of terrorism to produce fear in the target [15]. However, the major focus of this paper is the traditional terrorism.

2.3. Cyber Tools, Techniques Used by Terrorists

Terrorism has profited immensely from the technological and social advances of the 20th century, in terms of the level of destruction that can be created and the height of public anxiety it can spawn [16]. Terrorists take advantage of ICT due to its ability to improve communication and aid organization [17].

After the 9/11 attacks in the US an intensive discussion about the use of ICTs by terrorists began [18]. It was reported that the terrorists used the internet to prepare for the attack [19]. This is against the backdrop that the attacks were not cyber in nature, since it was not internet-based, yet the internet was used as one of the tools in the preparation [20]. The belligerent utilization of modern technology for management of information, communication and intelligence has had a progressive effect on terrorist activities. On their part, they continue to improve their sophistication and abilities in all aspects of operations and support using these tools [21]. Today it is a common knowledge that terrorists use ICTs and the Internet for recruiting, promoting propaganda, gathering of information, publication of training materials, communications, preparation of real-world attacks, terrorist financing, etc [22]. Terrorists are now known to plan and communicate with encrypted data even beyond law enforcement's ability to intercept or decode this data. They have utilized other ICT tools, including disposable cellular phones, over the counter long-distance calling cards, internet cafes, to mention but few. They even employ the use of embedding information in digital pictures and graphics [21].

3. Methodology

The research is explorative in nature, taking cognizance of the fact that while similarities may exist in terrorism trends worldwide, including in the use of tools and techniques, there are bound to be some practices, methods, tools, and techniques that are local, that is peculiar, to a terrorist organization.

Hence, focusing on traditional terrorism in Nigeria, with emphasis from year 2000 till date, the methodology used is first to highlight cyber tools and techniques used by terrorists to aid their activities. Secondly, we appraise the level of cyberspace utilization by Nigerian terrorists, after which Nigerian government's response to terrorism so far and its current capacity level in tackling the situation are assessed. Finally, recommendations on how terrorist activities in the country can be mitigated are given.

4. Findings and Discussion

4.1. Terrorism in Nigeria

Terrorism in Nigeria is a direct upshot of the people's deep disenchantment with their government. The mishandling of national issues has given rise to several dissenting groups along our geographical lines, including the Movement for the Emancipation of Niger Delta (MEND) in the South South; the Oodu'a People's Congress in the South West; the Bakassi Boys and the Movement for the Actualisation of the Sovereign State of Biafra in the South East, and the Jama'atu Ahlus Sunnah Lid Da'awati Wal Jihad, otherwise known as Boko Haram, in the North [23].

The core activities of these organizations have purely been in response to the inability of the society to meet their obligations, which is premised on perceived government's insensitivity to their needs. Over the years, terrorism trend in the country has moved from causes motivated by grievances that were purely socioeconomic to those majorly by religious fundamentalism.

Since the last decade, the scourges of MEND and Boko Haram have been felt in this nation at a magnitude never felt before. The October 1, 2010 Independence Day bombing of Abuja during the Golden Jubilee anniversary of Nigeria, claimed by MEND, readily comes into memory; and likewise, the spate of bombings claimed by the latter in Maiduguri, at the Police Headquarters and UN building in Abuja, Yobe, Adamawa, Kaduna, to mention but few, which culminated in the loss of many lives and property, cannot be overemphasized.

4.2. Terrorists' Exploitation of Cyberspace in Nigeria

No doubt, terrorists form a chunk, however small, of the country's population, and thus, a percentage of her cyberspace users. From observations, most of the activities of terrorists in the country are purely traditional terrorism. However, there were sparse occurrences of cyberterrorism activities where the telecommunication masts of some mobile network providers were attacked in some states [24]. Terrorists in Nigeria utilize the cyberspace for their activities, albeit not at an advanced level. Majorly, their exploitation has been limited to the usage of mobile technology for communicating between themselves and to media, and for planning, preparation, and coordination of attacks; and internet for propagating and communicating messages to the public.

For instance, prior to the October 1, 2010 bombing in Abuja, MEND used the internet to communicate their ploy to security agencies [25]. An individual who claimed to be a sympathizer of the Boko Haram group gained access into and posted online the profiles of more than fifty former and current State Security Service (SSS) officials, including the code number, appointment date, state of origin, bank account, to mention but few [26]. Some of these sympathizers are adept in the use of ICT, and it is not impossible for any to be providing logistic supports to the supported terrorist group.

Not too long ago, the Joint Task Force (JTF), a coalition of different security agencies mandated to curb insurgency, raided and recovered from the home of one of the leaders of the Boko Haram sect 54 assorted SIM cards. This is against the backdrop that the federal government has mandated all active SIMs to be registered [24]. It is evident the SIMs were used for communicating with the intention of identity hiding to avoid being easily tracked. For instance, a linear relationship between mobile subscriptions from July 2011 to February 2012 [27] and number of successful bombing operations by a terrorist group in Nigeria [28,29,30] was investigated, the correlation was 0.71. The question is, could there really be a relationship between these two variables? In May, 2013, mobile phone service was turned off in two among the states where the onslaught of the terrorist group were most [31]. Throughout the period this occurred there were no records of successful terrorist attacks. Not long after the service was restored the terrorist succeeded in launching some attacks.

Also, recently, terrorists have opted for the option of generating funds through cybercrimes. Foreigners are kidnapped, while the government or/and relatives of the kidnapped are contacted via mobile phones for ransom.

Intelligence reports have shown that there is a link between the Nigerian Islamist sect, Boko Haram, and the Algerian-based branch of al-Qaeda [32]. This means since the latter uses ICT for its operation it is natural for its protégé to follow suit.

4.3. Nigeria's Response to Terrorism

Nigeria is well known to fall short when it comes to emergency response. Taking proactive measures to forestall unwanted events is alien to the county. Signals are often ignored, warnings not paid due attention to.

In the case of response to terrorism, unfortunately, it has been through vicious suppression of opposition through the

use of force. In spite of this, the frequency of attacks, including suicide bombings has ceased to abate [23]. Rather, it has been on the increase. There have even been reports of extra-judicial killings by the military and other security agencies, all in their bid to quench insurgence [33]. Challenges including lack of capacity for quality operational intelligence gathering, lack of cooperation from local population, and lack of trust between government and its citizens [6] have all being hampering the prospect of success.

Generally speaking, the response to terrorism in Nigeria to a large extent has been on the defensive side, and mostly non-cyber in nature. While terrorism seems to have become a reality the country may continue to live with, it is unwise to remain on the defensive side of this menace – reacting only after every attack. An evidence of the federal government's lack of capacity to appropriately respond offensively to the abuse of cyberspace by terrorists is the ban of mobile networks in the most affected areas [31]. No doubt, this would have had negative effects on innocent people's ability to communicate online. Businesses in these areas too must have felt these effects.

On the part of the law making arm of the government, legislature, it has been a combination of lack of experience on general legislation, incapability of the part of some members, and lack of political will. These, and other reasons, explain why bills like the Cybersecurity and Information Protection Agency Bill was rejected by the House of Representative on the ground that it duplicated the efforts of some existing law enforcement agencies of the country [34]. Others alike, including the Computer Security and Critical Information Infrastructure Protection Bill 2005, the Cybersecurity and Data Protection Agency (Establishment, etc) Bill 2008, the Electronic Fraud Prohibition Bill 2008, the Nigeria Computer Security and Protection Agency Bill 2009, the Computer Misuse Bill 2009, and the Economic and Financial Crimes Commission Act (Amendment) Bill 2010 are all yet to become law [35].

It is surprising to know that the national security policy does not reflect present realities. The last review done was under the military regime in 1986, which led to the National Security Agencies Act [23]. In this present age, considering the rapidity of development in every facet of human endeavor, a 27 years old document, enacted by the military, would hardly be relevant to tackle present challenges in a democratic setting.

Also, Nigeria presently lacks capacities for digital forensics, internet filtering, to mention but few. There is also a lack of synergy among the security agencies. For instance, from videos posted online by some terrorist groups, using a voice recognition mechanism, the voice pattern of the speaker could be captured, and used to track the terrorist when next his voice traverses the cyberspace, say, through a phone call. Unfortunately, Nigeria lacks this capacity and required personnel.

5. Recommendations and Conclusion

It can be inferred that terrorist groups in Nigeria exploit the cyberspace to plan and coordinate their activities. This is more so, considering the fact that the survival of terrorism, in modern time, is largely due to the utilization of ICT. Terrorism thrives on unrestricted accessibility to some components on the cyberspace. This is one setback with ICT. Therefore, the battle to confront terrorism must begin at the cyberspace. A secure cyberspace will hamper the continuous boom and smooth running of terrorist activities. In other words, a secure cyberspace is an effective anti-terrorism measure.

Cybersecurity is the offensive way (otherwise known as a preventive measure) of combating terrorism. The security of the cyberspace is as crucial more than ever to the survival of mankind as the physical space is. This simply translates to the fact that the security of the cyberspace is not only necessary for the prevention of cyber attacks, but also physical and other forms of attacks that can be organized or coordinated via the cyberspace.

From a counter-terrorism point of view, cybersecurity, as a tool, is necessary for intelligence gathering.

5.1. Recommendations

It is unfortunate that despite all that the federal government has allegedly spent towards security, the nation is yet to have a true taste of it. For instance, in spite of money spent on deployment of CCTV cameras, the security agencies could not stop the June 16, and August 26, 2011 bombings of the Police Headquarters and United Nations Building respectively, in Abuja [36]. Beginning with the deployment of CCTV cameras only amounted to putting the cart before the horse. A CCTV camera would not detect a car containing bomb, neither does it recognise a terrorist by face.

Since this issue of terrorism is on a world scale, most of our recommendations are based on time-tested measures adopted by other countries, which have proved to be effective. These nations have gone beyond the stage Nigeria is now. We therefore solicit the following measures to ensure a safer Nigerian cyberspace:

i. Development of a cybersecurity culture [37]. Amongst most Nigerians today, information security generally does not receive due attention. For example, in the country today, it is a common knowledge that it is possible to purchase a registered SIM card. Many mobile phone users, when they lose their phones, often make little effort to block the registered SIM or recover it. They find it easier to purchase and register a new one. The stolen SIM can easily be sold by the robber, which can then be used to perform illegal activities. There is need for proper awareness on the part of the authorities concerned on issues and challenges associated with information and communication technologies (ICT) deployment, uses and misuses.

ii. Development of Cybersecurity Policies and Strategies [38]; and ensuring that necessary legislative and legal

frameworks are put in place. These are borne out of strong political will.

iii. Establishment of a rapid information exchange system [39]. Presently in the country, reporting terrorists' plans via use of mobile phones have proved to be unsafe. There have been cases of informants being found out and assassinated by terrorists. The nation needs a more secured communication infrastructure to guarantee a secure information channel.

iv. Cyberspace patrol. This includes policing of crimes in social networks and virtual worlds. It may require monitoring and surveillance of websites whose materials are harmful to the security of the nation. If need be, access to these sites could be completely restricted.

v. Ethical utilization, more research into and development of other offensive and defensive cyber capabilities, for instance, digital forensics, communication interception, accessing and analysis of call data or traffic records, phone hacking.

vi. Collaborations and co-operations with other countries.

Other recommendations, considering the present level of the national attitude to the security of the cyberspace, include:

i. Government must intensify SIM registration of mobile phone users. Activities of agents that deal in assorted SIM cards should be rigorously clamped down on and necessary frameworks to deal decisively with offenders put in place.

ii. Collaborations between government and network (GSM and internet service) providers should be harnessed.

iii. Monitoring of the cyber cafes, especially in areas that have been discovered as hotspots for terrorists. Presently, there are no regulations for regulating activities of internet cafés in Nigeria. Unfortunately, these are easy avenues for communication for terrorists.

iv. Establishment of a centrally-managed crime database to serve all security agencies. Presently, there is no proper coordination among security agencies in the country in the handling of terrorists' cases.

v. Intelligence reports gathered so far can be used to design a honey pot website to lure and keep eye on the activities of terrorists [40].

5.2. Conclusion

One can infer that terrorists' use of the cyberspace in Nigeria is still at a relatively non-advanced stage. But considering the rate at which there are potentials for growth in sophistication, it may not be long to see a commensurate level rise in cyberspace utilization.

There is need to ask the questions, how secure is the country's cyberspace? How far is she willing to go to ensure this security? How much manpower is available? How much is allocated for the security of the space in the budget? How much security has this ensured? There is need to weigh the consequences of the infiltration of the present level of security of the cyberspace, and estimate the future consequences if adequate anti-terrorism measures are not put in place. For example, as more people get access to the internet, and nothing concrete is done in respect of its security, more sympathisers of terrorist groups could adopt 'do-it-yourself terrorism' [41], having laid hands on materials to develop needed tools online.

The initiative of the federal government to deploy a ₦10 billion infrastructure, fashioned along the line of the Global System of Telecommunications (GSM), with a capacity to detect threats, meant for the security services, under the National Public Security Communication System is a drive in the right direction [42]. We believe that with adequate budgetary allocations, enhanced cooperation and integration of all tools [16], infrastructure, and right collaborations, Nigeria can successfully tackle terrorism.

REFERENCES

[1] " Terrorism", Retrieved from http://en.wikipedia.org/wiki/Terrorism#Tactics

[2] www.itu.int

[3] Internet Crime Complaint Center, "2010 Internet Crime Report." Retrieved from www.ic3.gov/media/annualreport/2010_ic3report.pdf

[4] Oyeniyi, A. B. (2010). Terrorism in Nigeria: Groups, Activities, and Politics. *International Journal of Politics and Good Governance*, Volume 1, Number 1.1 Quarter 1, ISSN No. 0976 – 1195

[5] Boye, R. R. Nigeria Anti-Terrorism Law and Global Security. Retrieved on November 3, 2013 from http://www.aceser.net/journals/download.php?aid=42&action=download

[6] Forest, J. J. F. (2012). Confronting the Terrorism of Boko Haram in Nigeria. Retrieved on October 24, 2013 from http://www.jamesforest.com/wp-content/uploads/2012/06/Boko_Haram_JSOU-Report-2012.pdf

[7] Hashim, A. S., Patte, G., and Cohen, N. (2012). 'Western Ways Are Evil': The Emergence and Evolution of Boko Haram. *Counter Terrorist Trends and Analysis*, Vol. 4 Issue 7. Retrieved on October 24, 2013 from http://reliefweb.int/sites/reliefweb.int/files/resources/CTTA-July12.pdf

[8] Ajayi, A. I. (2012). 'Boko Haram' and Terrorism in Nigeria: Exploratory and Explanatory Notes. *Global Advanced Research Journal of History, Political Science and International Relations*, Vol. 1(5) pp. 103-107.

[9] International Telecommunication Union (2004), "Understanding Cybercrime: A Guide for Developing Country." Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[10] Magutu, P.A., Ondimu, G.M., and Ipu, C.J. (2011), Effects of Cybercrime on State Security: Types, Impact and Mitigations

with the Fiber Optic Deployment in Kenya, Journal of Information Assurance & Cybersecurity, DOI: 10.5171/2011.618585

[11] Nojeim, G.T. (2009), Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace. Statement Before the Senate Committee on the Judiciary, Subcommittee on Terrorism and Homeland Security.

[12] Cybercrime Law, "Peace, Justice and Security in Cyberspace." Retrieved from http://www.cybercrimelaw.net/Cybercrimelaw.html

[13] Heickero, R. (2008). Terrorism Online and the Change of Modus Operandi. Retrieved August 24, 2013 from http://www.dodccrp.org/events/13th_iccrts_2008/presentations/209.pdf

[14] Zalman, A. Types of Terrorism: A Guide to Differenct Types of Terrorism. Retrieved August 24, 2013 from http://terrorism.about.com/od/whatisterroris1/tp/DefiningTerrorism.htm

[15] Murill, R. (2011). The Question of Cyber Terrorism. Retrieved August 24, 2013 from http://articles.forensicfocus.com/2011/07/23/the-question-of-cyber-terrorism/

[16] U.S. Department of Justice, Federal Bureau of Investigation (1999), "30 Years of Terrorism", Retrieved from www.fbi.gov/stats-services/publications/terror_99.pdf

[17] "Weapons & Terrorism: Terrorist Use of Information Technology." Retrieved from http://www.terrorismfiles.org/weapons/information_technology.html

[18] Lewis, "The Internet and Terrorism." Retrieved from http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; Lewis, "Cyber-terrorism and Cybersecurity"

[19] Weimann, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning," 2003, Retrieved from http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, Retrieved from http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;

[20] CNN, News, 04.08.2004. Retrieved from http://www.cnn.com/2004/US/08/03/terror.threat/index.html

[21] "What is terrorism?" Retrieved from http://www.terrorism-research.com/

[22] International Telecommunication Union (2004), "Understanding Cybercrime: A Guide for Developing Country." Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[23] "Responding to Terrorism in Nigeria." Retrieved from http://234next.com/csp/cms/sites/Next/News/National/5743941-146/responding_to_terrorism_in_nigeria.csp

[24] Adeyemi, K., Joel, D., Tsenzughul, A. (2012). Gunmen Attack MTN, Airtel masts in Kano, Borno, Bauchi, Yobe. The Nation Newspaper. Retrieved September 6, 2012. Retrieved from http://www.thenationonlineng.net/2011/news/60494-gunmen-attack-mtn-airtel-masts-in-kano-borno-bauchi-yobe.html, published in September, 2012.

[25] Jeremy W., "Nigeria Explosion: Independence Celebrations Marred By Violence." Retrieved from http://www.csmonitor.com/World/Africa/Africa-Monitor/2010/1001/Nigeria-explosion-Independence-celebrations-marred-by-violence, published on October 1, 2010

[26] Sahara Reporters, "Boko Haram Sympathizer Obtains Personnel Records of SSS Employees and Posts Them Online." Retrieved from http://saharareporters.com/news-page/boko-haram-sympathizer-obtains-personnel-records-sss-employees-and-posts-them-online?page=2, published on August 30, 2012.

[27] www.ncc.gov.ng

[28] Nairaland Forum, "Boko Haram Updated Timeline of Terror." Retrieved from http://www.nairaland.com/854885/boko-haram-updated-timeline-terror, published in November 27, 2012.

[29] Human Rights Watch, "Spiralling Violence: Boko Haram Attacks and Security Force Abuses in Nigeria", ISBN: 1-56432-951-8, 2012.

[30] Muhammad L. (2012). "Terrorism in Nigeria: Timeline between 26.08.2011 and 26.04.2012 by Wale Babatunde." Retrieved from http://muhdlawal.wordpress.com/2012/04/27/terrorism-in-nigeria-timeline-between-26-08-2011-and-26-04-2012-by-wale-babatunde/, published in April 27, 2012.

[31] Abdullahi, T. A., Hamza, I., Yahaya, I., Hamisu, K. M., and Zakariyya, A (2013). "Cell phone service cut in Borno, Yobe", Daily Trust Newspaper, May 17, 2013.

[32] The Nation Newspaper, "Bokom Haram Has Links with al-Qaeda – Algerian Minister." Retrieved from http://www.thenationonlineng.net/2011/index.php/news-update/26240-boko-haram-has-links-with-al-qaeda-algerian-minister.html, published on November 16, 2011.

[33] Human Rights Watch (2011), "A Human Rights Agenda for Candidates in Nigeria's 2011 Elections." Retrieved from http://www.hrw.org

[34] Daily Champion Newspaper, "Nigeria: Representatives Reject Cyber Bill." Retrieved from http://allafrica.com/stories/201103020802.html, published on March 2, 2011.

[35] ThisDay Newspaper, "Non-Passage of Cyber Crime Bill Decried." Retrieved from http://www.thisdaylive.com/articles/non-passage-of-cyber-crime-bill-decried/88750/, published on March 31, 2011.

[36] Oludare O., "Terrorism in Nigeria: Our Preparedness and Exposure Reduction Since October 1, 2010 Bombing." Retrieved from http://saharareporters.com/article/terrorism-nigeria-our-preparedness-and-exposure-reduction-october-1-2010-bombing.

[37] Stein S., Solange G. (2011), "A Global Treaty on Cybersecurity and Cybercrime." Retrieved from http://www.cybercrimlaw.net

[38] Igli T., Solange G. (2011) Ghernaouti-Hélie; "Information security evaluation: a holistic approach", EPFL Press

[39] Colonel S.S. Raghav, "Cyber Security in India's Counter-Terrorism Strategy." Retrieved from ids.nic.in

[40] Theohary, C.A. and Rollins, J. (2011), "Terrorist Use of the Internet: Information Operations in Cyberspace",

Congressional Research Service.

[41] Liang, C.S. "Terrorism, Organised Crime and Cyber Security." Retrieved from http://www.gcsp.ch/New-Issues-in-Security/Training-Courses/13th-New-Issues-in-Security-Course-NISC/NISC-Outline-and-Curriculum-2012/Week-11-Terrorism-Organised-Crime-and-Cyber-Security-Christina-Schori-Liang

[42] Vincent Ikuomola, "Government to Fight Boko Haram, Others With ₦10b Gadgets", published on The Nation Newspaper of November 16, 2011.