2018

Countering Expansion and Organization of Terrorism in Cyberspace

Sunday Oludare Ogunlana
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Sunday Oludare Ogunlana

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Olivia Yu, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Karen Shafer, Committee Member,
Public Policy and Administration Faculty

Dr. Eliesh Lane, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Countering Expansion and Organization of Terrorism in Cyberspace

by

Sunday Oludare Ogunlana

MS, University of Maryland University College, 2014

BS, University of Maryland University College, 2012

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Homeland Security Policy and Coordination

Walden University

November 2018

Abstract

Terrorists use cyberspace and social media technology to create fear and spread violent ideologies, which pose a significant threat to public security. Researchers have documented the importance of the application of law and regulation in dealing with the criminal activities perpetrated through the aid of computers in cyberspace. Using routine activity theory, this study assessed the effectiveness of technological approaches to mitigating the expansion and organization of terrorism in cyberspace. The study aligned with the purpose area analysis objective of classifying and assessing potential terrorist threats to preempt and mitigate the attacks. Data collection included document content analysis of the open-source documents, government threat assessments, legislation, policy papers, and peer-reviewed academic literature and semistructured interviews with fifteen security experts in Nigeria. Yin's recommended analysis process of iterative and repetitive review of materials was applied to the documents analysis, including interviews of key public and private sector individuals to identify key themes on Nigeria's current effort to secure the nation's cyberspace. The key findings were that the new generation of terrorists who are more technological savvy are growing, cybersecurity technologies are effective and quicker tools, and bilateral/multilateral cooperation is essential to combat the expansion of terrorism in cyberspace. The implementation of recommendations from this study will improve the security in cyberspace, thereby contributing to positive social change. The data provided may be useful to stakeholders responsible for national security, counterterrorism, law enforcement on the choice of cybersecurity technologies to confront terrorist expansion, and organization in cyberspace.

Countering Expansion and Organization of Terrorism in Cyberspace

by

Sunday Oludare Ogunlana

MS, University of Maryland University College, 2014

BS, University of Maryland University College, 2012

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy Administration

Homeland Security Policy and Coordination

Walden University

November 2018

Dedication

I dedicate the dissertation to the memory of my Late grandparent, Pa. Samuel Ayinla Adepoju and Mother-in-Israel Sarah Anike Omisande Adepoju. They were and remain the source of love and strength for me today. They planned my life to excel academically even though none of them had the opportunity of going to school. They conceived the dream, and the idea became a reality with the completion of this program. They inspired me to go to school even when there was no hope we will have money to pay the school fees. I am laid under the debt of everlasting gratitude.

Acknowledgments

To God Almighty, the beginning, and end of all things which gave me strength from the start to the end. To my dissertation committee Chair, Dr. Olivia Yu: Thank you for your advice, patience, guidance, and professionalism. I made it because of your tutelage. I am forever grateful.

To my Dissertation Committee members, Dr. Karen Shafer, who exposed me to qualitative study during my second residency. Thank you for your encouragement and for being part of my journey. It was a pleasure to work with you. I would like to thank Dr. Eliesh O'Neil Lane, the University Research Reviewer for keeping me within the strict academic tracks of a true scholar.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Information communication technology (ICT) is a new tool of attack in the hand of terrorist organizations. Indeed, terrorism is about information. Although ICT has expanded opportunities for personal connection, interaction, and dissemination of information from every part of the world, it has introduced new vulnerabilities that terrorists exploit to cause harm to societies, including the spread of violent religious ideology and mobilization (U.S. Army Training and Doctrine Command, Assistant Deputy Chief of Staff for Intelligence-Threats [DCSINT], 2006). The present danger is that modern-day terrorists have transformed ICTs into tools of attack with weaponized information. Terrorist websites serve as the virtual training ground that host messages and propaganda videos that help to boost morale and networking, and drive fundraising efforts, recruitments, and call for terror actions. Kaplan (2009) pointed out that terrorist websites moved from fewer than 100 to 4,800 between 2006 and 2008. The organizations attract attention by posting roadside bombing, and a significant portion of society views the decapitation of hostages and terror propaganda videos. In fact, some jihadist websites have video games where users pretend to be holy warriors killing government soldiers. Hence, cyberterrorism has become a new focus because of the technology's interface functionality, which makes it simple and efficient to accomplish terrorists' goals. In Nigeria, terrorist organizations have shifted the battle to cyberspace, using social media platforms to coordinate attacks, communicate, and spread messages of hate and violent religious ideology. Different countries, including Nigeria, used several kinds of technologies to mitigate the effect of the terrorists' harmful messages in cyberspace.

Therefore, a need exists for a study to understand the effectiveness of those cyber technologies and how security experts and administrator make their choices. The potential social implication of this study is that the outcome of the research will help public law enforcement and intelligence community in Nigeria to build capacity, using relevant cybersecurity technologies to confront a series of cyber threats, especially terrorist propaganda.

The 21st-century terrorists are acquiring technological skills that enable them to engage in extremely destructive acts such as cyberterrorism, the spread of new doctrines and falsehood, blackmail, and exploitation, undergirded by extreme religious ideologies that are currently affecting the spectrum of conflict. Terrorists' chief motive is to use fear to compel their targets to comply with their demands or ideologies (DCSINT, 2006).

The term *cyberterrorism* is a compound of the words *cyberspace* and *terrorism* (Minei & Matusitz, 2012; Ogun, 2012). The Federal Bureau of Investigation (FBI) describes *cyberterrorism* as any criminal activities perpetrated with the aid of computer systems and telecommunication networks with the intention of provoking violence, including destruction and disruption of services. Hence, the terrorists' agenda is to create excessive fear as a result of confusion and dilemma within a given group or community, with the goal of coercing a government or population to conform to their political, social, or ideological demand (Al-Mazari, Anjariny, Habib, & Nyakwende, 2016; Ogun, 2012). The Department of Homeland Security (DHS) stated that terrorism is:

> . . . [An] activity that involves an act that: is dangerous to human life or potentially destructive of critical infrastructure or key resources; and . . . must also

> appear to be intended to (i) intimidate or coerce a civilian population; (ii) influence the policy of a government by intimidation or coercion; or (iii) affect the conduct of a government by mass destruction, assassination, or kidnapping. (Schweitzer, 2005)

Cyberspace is the new territory where terrorist organizations incite violence. The ways in which terrorists disseminate information to spread hate and violent religious messages to radicalize young people have assumed new dimensions in the last 10 years. Experts have pointed out that Twitter was the most popular platform among terrorist organizations. The British Jihadis working for ISIS in Syria threaten the United States of America (Berger, 2015) using Twitter. The attack on July 26, 2016 in France, where terrorists took nuns and worshipers hostage and slit the throat of an 85-year-old priest, is a point of reference. The investigation established the fact that the two attackers involved were directed and stimulated by ISIS propagandist Rachid Kassim through an encrypted chat room on the digital application Telegram (Homeland Security News Wire, 2017). Social media has fueled the recent upsurge of lone wolf terrorism around the world (Aly, Macdonald, Jarvis, & Chen, 2017; Berger, 2015).

The ISIS has a significant influence on most of the terrorist organizations operating from Africa, including the notorious Boko Haram (Jamā'a Ahl al-sunnah li-da'wa wa al-jihād), a Sunni group preaching religious extremism and Jihad in Nigeria. The group renamed itself as "Islamic State's West Africa Province" (ISWAP) in April 2015. The ISIS has taken over the propaganda function of Boko Haram against the Nigerian State, using advanced technology such as encrypted media such as Telegram to

pass messages among members about clandestine operations. The group is using social media to recruit members and raise money for its activities, including the spread of violent ideologies (Baken, 2013; Hamin et al., 2016; Musa, 2012). The organization uses YouTube to broadcast its activities as a way of threatening people with messages of fear to force the Nigerian government to concede to its demands. For instance, Boko Haram used YouTube to announce the abduction of more than 276 schoolgirls in 2014. The group usually uses YouTube videos to distribute jihadist sermons in northern Nigeria, calling people to deny girls modern education because women are slaves according to their ideology (Maiangwa & Agbiboa, 2014).

In Chapter 1, I will present further background on the threat of terrorist propaganda in cyberspace and possible control mechanisms. Also, I delineate this study's problem statement, purpose, research questions, theoretical framework, nature, definitions, scope and delimitations, limitations, and significance.

Background

The militarized response to 9/11 and the global war on terror forced terrorist organizations to withdraw from physical terrain and establish a significant presence in cyberspace (Weimann, 2014). Initial steps taken by terrorist groups included creating several websites to establish their presence and propagate their agenda. Terrorist organizations are sharing knowledge and imitating one another in their operations with Nigeria's Boko Haram, mirroring the global terrorist network in the act of spreading their version of their ideology in cyberspace. Cyberspace has become a new battleground with

governments all over the world in search of a solution with adequate cyber intelligence to confront and destabilize terror infrastructures.

In April 2016, some sects of pro-ISIL cyber groups announced the formation of the United Cyber Caliphate (UCC) with the sole aim of training other jihadist groups on how to use social media technologies to propagate their ideology (Flashpoint, 2016). The UCC Coalition includes the Cyber Caliphate Army, Sons of the Caliphate Army, the Ghost Caliphate, and the Kalashnikov Team. In fact, the pro-ISIL group continues to develop cyber capabilities to the extent that in January 2015, the group hijacked the U.S. Central Command Twitter account and posted unusual tweets and images that misrepresented the Department of Defense (CNN, 2015).

Furthermore, these terrorist organizations migrated to social media platforms such as Twitter, Facebook, Telegram, YouTube, Instagram, and WhatsApp after intelligence and law enforcement agencies brought down all their websites (Weimann, 2014). Approximately 90% of terrorist communication now takes place on social media. The use of images and Internet videos has far reaching effects on their targets with the purpose of inciting fear, anger, and overreaction (Minei & Matusitz, 2012). Internet-aided terrorism, such as the dissemination of misleading terrorist information to trigger feelings of panic and overreaction, remain a public threat that requires solution.

The unique borderless nature of cyberspace makes it difficult to monitor, unlike traditional land borders. New media technologies have made it possible to communicate with, manipulate, and control the minds of total strangers using special media effects. Hence, the information revolution is altering the nature of conflict. Cyber terrorists use

social media to communicate with each other and the entire world (Flashpoint, 2016; Ogun, 2012). The implication is that a terrorist can send a message to a target stranger thousands of miles away, thereby strengthening their network and affording them the advantage of bypassing traditional forms of communication. The anonymous nature of the Internet makes it difficult to identify the actor. Also, the laws that govern cyberspace differ from one country to another. Whereas some countries have adequate legislation to punish offenders, others do not have such laws that can curb the abuse and misuse of the Internet and social media.

Terrorists' influence on social media has created homegrown terrorists who are self-recruited and connected with other members globally. Research has documented that future generations of terrorists will be sophisticated with the use of new media technologies to cause extreme damage (Minei & Matusitz, 2012). In fact, modern-day terrorists are not products of poverty and ignorance but self-recruited radicals without leadership (Sageman, 2008).

The United States has been cautious about deploying offensive technologies against terrorists because of the fear that this could push state actors such as Russia and China to develop countermeasures. However, research suggests that more effort should be devoted to countering terrorist narratives in cyberspace (Barnes, Fidler, Lubold, & Shishkin, 2015). Also, a study conducted to determine how terrorists use the Internet revealed that terrorist organizations use the Internet for different purposes but use social media to propagate their ideology, and they are quickly adapting to the use of technology as a mode of transnational operation (DCSINT, 2006; Ogun, 2012). In fact, the Internet

via social media technologies has become the main source of communication to exploit the populace. The method and mode of communication are yielding their desired result as ISIS has used social media to influence sympathizers to take action against the people in their home countries.

Research suggests that the legal use of control mechanisms to make it difficult for terrorists to have easy access to the Internet could lessen the effect of incisive terror messages (Ogun, 2012). Furthermore, the service providers of social media platforms such as Facebook, Twitter, and YouTube should become proactive by banning those offensive messages on their platforms (Ogun, 2012; Schechner, 2015). The Facebook social media company claims it has suspended more than 125,000 user accounts and shut down 360,000 with connections to extremist ideologies in 2015 (Isaac, 2016).

Researchers have uncovered that cyberspace has become a new "safe haven" for terrorist organizations with the ability to use sophisticated technology for communication to lure new members and manipulate the public by reaching out to a mass audience (Ogun, 2012; Sageman, 2008; Weimann, 2014).

Knowledge of how terrorist groups have migrated to cyberspace indicates clearly that it has an adverse effect on the society and global security. Terrorists use sophisticated technology to create an atmosphere of uncertainty, panic, and, in some instances, force a government to a concession. Young people are being increasingly influenced through messages on social media to act against their home countries. The strategic use of new media technologies by terrorists has negative social effects because of their ability to persuade and influence people's minds. Counterterrorism experts

around the world have published several pieces of research on how to target the "mind and heart" of youth through counter-narratives on the Internet. However, the experience of how to use sophisticated technology against terrorists has not been documented in the literature. Hence, the research evaluated the practicality of technology among other traditional approaches to mitigate the organization and expansion of terrorism in Nigeria cyberspace, using acceptable international best practices. A theoretical model that supports this application is Cohen and Felson's (1979) routine activity theory (RAT). I expand on this later in this chapter and in Chapter 2.

Problem Statement

Terrorist propaganda and networking in the Nigerian cyberspace give rise to the question of what measures that Nigerian government agencies should take to mitigate the effects of terrorist propaganda in cyberspace. I used a qualitative interview design to explore the perceptions of security experts on the topic of cybersecurity technologies, including its effectiveness and practicality in alleviating terrorist propaganda and networking in cyberspace. Cyberspace is increasingly becoming the platform to promote terrorism because it allows easy access to actors to disseminate information beyond geographic borders (Berger, 2015; Hamin, Othman, & Selamat, 2016; Osho & Onoja, 2015; Weimann, 2014). The Internet and social media create alternative realities for actors, and audiences and users are influenced by the information given to them by strangers (Waltzman, 2017). Terrorists' use of websites, blogs, YouTube, Twitter and Facebook to influence people is on the rise globally, and the security community has not developed systematic measures to mitigate terrorist activities such as the manipulative

use of new channels to influence the public (Musa, 2012; Oluwafemi, Adesuyi, & Shafi'i, 2013). As Boko Haram, a Nigerian militant Islamist group, has embraced technology for spreading violent religious ideology and hate messages, raising money, conspiring, planning, and executing their attacks (Baken, 2013; Hamin et al., 2016; Musa, 2012), the Nigerian government has just begun to incorporate robust active and passive defense measures against adversaries into the National Security Strategy.

Research supports the notion of governing cyberspace using traditional models of law enforcement, including the enactment of legislation to deal with cybercrime, including other related offenses (Adomi & Igun, 2008, p. 718). Also, the literature suggests that the future of fighting extremism, falsehoods and bogus information in cyberspace would rely on robust technology and how it is deployed (Berger, 2015, p.15). There is little information on how the experts make their choice of cybersecurity technologies that can be used effectively to halt the expansion of terrorism in cyberspace and the extent to which the expertise should be used.

Purpose of the Study

My purpose in this qualitative interview study was to gain an understanding of how experts and security administrators choose cybersecurity technologies to mitigate terrorist propaganda and networking in Nigeria cyberspace. The qualitative interview study focused on experts from five sectors (Law enforcement, Intelligence, Military, Academic, and private sector) in Nigeria.

Research Questions

1. How do the experts see the role of technology in fighting expansion and organization of terrorism in cyberspace?
2. How do experts perceive the effectiveness and practicality of cybersecurity technologies as a tool to mitigate terrorist propaganda and networking in cyberspace?

Theoretical Framework for the Study

The theoretical framework for this study is Cohen and Felson's (1979) RAT, which is an environmental, place-based account that three elements must be available for a crime to occur: opportunity, motivation, and platform. Miró (2014) explained that the absence of protectors who are competent to defend the target and victims create an opportunity for the willing potential lawbreaker with a capacity to commit a crime. Several crime prevention methods are based on actor choice. Based on the research question, RAT will enable the researcher to understand how terrorists make their decisions to use cyberspace for terror activities and how the choice of suitable cybersecurity technologies can frustrate them and decrease their motivation.

Social media provides a convenient and cheap platform for terrorist organizations to communicate and spread the radical ideology of violence, recruit members, and coordinate and execute their terrorist plans (Holt, 2016). Terrorists' capability to remain elusive in cyberspace makes them beneficiaries of ICTs (Schultz, 2015). However, it is possible to stop them from gaining access to the protection that cyberspace offers them. Hence, governments, intelligence organizations and law enforcement actors must devise

counter-measures to stop terrorists from hijacking social media to serve their nefarious purposes. The Internet was designed for legitimate use without envisioning the security challenges that it poses today. In fact, the emergence of social media platforms creates new opportunities for terrorists to communicate without hindrances and further poses new challenges for law enforcement and intelligence organizations (Dean, Bell, & Newman, 2012). Meanwhile, the vast majority of cyberspace belongs to the public for individuals, businesses, and governments using it for legitimate purposes. In today's world, terrorists spread radical ideologies and violent messages to threaten populaces and recruit members into their fold. The prevalence of social media platforms such as Facebook, Twitter, Instagram, and WhatsApp, which create real-time constant connectives, has serious implications for cyber security (Rogers, 2016).

Hence, there is a need for technologically based techniques to detect, prevent and stop terrorists from manipulating the public. Eliminating or restricting terrorists' access to cyberspace will deny them the opportunity of virtual recruitment and further stop them from perpetrating radical ideologies online. Research can provide insights into how the government can develop strategies based on RAT to deny terrorists access to cyberspace, using efficient technologies to block terrorist propaganda that usually leads to recruitment and self-radicalization. Despite Barlow's (1996) assertion that cyberspace is free and independent as stated in the Declaration of the Independence of Cyberspace, the nation can balance against potential harms that threaten its stability, including the use of technology to deter terrorists from cyberspace.

Nature of the Study

The nature of the study was a qualitative research interview methodology with a focus on how the Nigerian government manages terrorist organizations networking and propaganda in the cyberspace. In this study, I obtained individual experts' perceptions about the effectiveness and integration of cybersecurity technologies with counterterrorism strategy to stop terrorists' propaganda campaign and networking in Nigeria cyberspace. Exploring the perceptions of experts and security administrators will require detailed and in-depth information and analysis of their thinking and decision-making processes. I collected empirical data on the situational factors and the thought and the decision-making processes of experts by performing secondary data analysis and undertaking in-depth and intensive in-person interviews with known security experts. I examined the phenomenon through interviews with key public and private sector individuals. Also, I reviewed relevant documents such as legislation, executive orders, research papers, and transcripts of public speeches by government officials. Qualitative research interviews were appropriate for this project to grasp the complexity and individuals' differences of how experts respond to the challenges of cyberterrorism, using cybersecurity technologies especially the mitigation of terrorists' communication and networking in the cyberspace. Networking by terrorist organization in cyberspace is a contemporary issue not limited to Boko Haram in Nigeria. Therefore, Nigeria, as well as other nations in the region, is developing strategies to cope with cyber risk based on information from international organizations, highly developed partners, and vocal private sector actors.

Assessing effectiveness and practicality of cybersecurity technologies in mitigating terrorists' networking and propaganda in Nigeria's cyberspace based on perceptions of experts enabled researchers to identify areas where improvements are required. Second, strategy is not a topic that lends itself to experimentation. The application of strategy involves significant organizational commitment. It is impossible to control variables on the technical sophistication of a nation's workforce or manipulate the number of connections to the Internet. As the cyber world grows daily, the threat landscape is changing, which increases the risks to governments and individuals simultaneously. Therefore, I answered the research question using a qualitative research interviews method.

Definitions

Artificial intelligence (*AI*): The science and engineering of creating intelligent machines, particularly intelligent or smart computer programs that perceive its environment well enough to identify events and take action against a predefined purpose. (Korolov, 2017; Lee, 2015).

Counterterrorism: The use of personnel and resources to preempt, disrupt, or destroy the capabilities of terrorists and their support networks. It is an offensive approach to threat, involving diplomacy, intelligence operations, law enforcement, military operations, and counterterrorism training (Sandler, 2015, p. 13).

Cyberspace: The global domain in the information environment, which consist of the interdependent network of information technology infrastructures, including the

Internet, telecommunications networks, computer systems, and embedded processors and human users that interact with these systems (Ottis & Lorents, 2010).

Cyber intelligence: Tracking, analyzing and countering of digital security threats. This type of intelligence is a blend of physical espionage and defense with modern information technology (Goel, 2011, p.133).

Cybersecurity: Set of practices, policies, training, and technology designed to protect the cyber environment and ensure its integrity and usability (Oluwafemi et al., 2013, p. 106).

Cyberterrorism: Terrorists use cyber technologies to recruit, train, plan, and fundraise. The motivation is to instill fear so that targets will comply with demands or ideology (Ogun, 2012, p. 208).

Cyberterrorist: Cyber actors or groups with a direct or indirect association with a formally recognized terrorist group (Denning, 2000, p. 3).

Information communication technologies (*ICTs*): All devices, including networking components, applications, and systems, which enable people and organizations (i.e., businesses, nonprofit agencies, governments and criminal enterprises) to interrelate in the digital world. (Eriksson & Giacomello, 2006; Jacob, & Akpan, 2015; Oluwafemi et al., 2013; Olusola, Samson, Semiu, & Yinka, 2013).

Information warfare: The use of computer technology as a weapon in political conflicts, espionage, and propaganda. It is stealthy and difficult to detect (Goel, 2011, p. 134).

Intelligence readiness: A state of the optimal organization and procedural conditions put in place to manage all sorts of security threats, including cyber through information management for timely intervention, expert analysis, tailored synthesis, and provision of support to consumers (Goldman, 2011).

Propaganda: Misleading information or publicized biased view, which is useful to promote a certain political cause (Minei & Matusitz, 2011, p. 997; Ogun, 2012, p.203).

Technological surprise: A unilateral influence gained by the introduction of a new weapon or the use of a known weapon in an innovative approach toward an adversary who is either ignorant of its existence or not ready with adequate countermeasures (Goldman, 2011).

Terrorism: Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents (Sandler, 2015, p.3).

Terrorist organizations: Any group practicing, or that has significant subgroups that practice, international terrorism (Hoffman, 2006, p.5).

Assumptions

The philosophical assumptions underpinning this qualitative interview study design were rooted in the constructivist tradition, which conceives the meanings of reality (ontology) as varied and multiple, making researchers look into the complexity of opinions instead of reducing them to a few categories (Goduka, 2012). Participants' perspectives varied and complex and the study gained their subjective meaning through interviews about the role of cybersecurity technologies in fighting the expansion of terrorism in cyberspace. The participants' testimonies were triangulated with document

content review, which was processed through the application of the program level analytical model to bolster credibility and confirmability.

In terms of the nature of knowledge (epistemology), the truth is relative, and it depends on individual perspectives. Individuals seek to understand the world in which they live and to develop the subjective meanings of their experiences (Creswell, 2009). Hence, the knower and the known are connected to each other (Gelo, Braakmann, & Benetka, 2008). Lived truths were revealed through the analysis of the subjects' beliefs in the social dynamics compared with the evidence concerning the mitigation of the terrorist threat in the cyberspace.

I explored the terrorism phenomenon through a routine activity theoretical lens and social action that makes proper guardianship of cyberspace to reduce the motivation of potential cyberterrorists. In this study, I focused on the role of technologies that protect and prevent the expansion of terrorism in cyberspace, including how experts select those tools. The interpretive analysis assumes that an objective view of the role of technologies could be achieved through adherence to facts provided by Nigerian security professionals who were protected by a stringent interview protocol. Also, the qualitative interpretation was applied to identify suboptimizations in the planning process and the essence of the research questions. These views allowed for the generation of meanings based on the interactions with the sample population. My goal in the research was to study participants' views of the phenomenon under study, which enables the researcher to understand their action as related to the topic (Baxter & Jack, 2008).

Constructivism also supports the adoption of qualitative research methods with narratives, phenomenology, grounded theory, ethnographies, and case study designs as well as the use of in-depth interviews with open-ended questions to allow participants to share their views (Creswell, 2009). My role as the researcher was to reconcile the meaning of the participants' experiences through personal interpretations, but the phenomenon is presented from a security perspective, not from individual perspectives.

Consequently, I assumed a constructivist and a subjectivist worldview to understand how experts perceived the effectiveness of cybersecurity technologies in fighting the organization and expansion of terrorism in Nigeria cyberspace.

Scope and Delimitations

The scope of this study included an examination of how Nigerian government manages terrorist organizations networking and propaganda in the cyberspace. The study was delimited to qualitative interviews bounded by time and location in Nigeria between May to June 2018. I focused the theoretical lens on relevant issues in Nigeria counterterrorism campaign and cybersecurity strategy. This qualitative research interviews encompassed security experts; institutions, including public and private agencies responsible for the protection of the Nigerian cyberspace against adversaries. The purposive sampling of fifteen security administrators limited the scope of the qualitative inquiry.

The scope of this study did not include intelligence gathering techniques, and the assumption was based on constructivist word view that generates meaning and knowledge from the interaction between selected population experiences and ideas. The

choice of Nigeria as the scope of the study was appropriate because terrorist groups operate, using the Nigerian cyberspace as a platform for communication and social media technologies as a medium for spreading radical ideology. Hence, the study appraised the effectiveness of technology to mitigate terrorist propaganda and networking in cyberspace in the context of Nigeria from the eyes of the law enforcement, policymakers, Intelligence personnel and security administrators. The strategy was tailored to the unique circumstances of the country in scope.

Limitations

The research used data and studies available in public domain and did not delve into sensitive classified information. Some aspects of the report concerning the area of cyber weapons are classified and was not be available to most researchers. Any information designated as sensitive when released has potential to harm security and may represent an unjustified invasion of privacy. This limitation would not impede the relevance of this qualitative research interviews study. My background in cybersecurity had no relevant biases or conflicts of interests that would affect my role of researcher as an independent observer. I mitigated this limitation by maintaining an open mind to opposing theories and contrary evidence without a preconceived solution to the problem.

Also, a significant risk of a qualitative design is that the subject of the study may not be representative. Qualitative research interviewing method of data collection has the potential for subconscious bias and inconsistency. Hence, some of the limitations that the study might have encountered was the participant ability to understand the questions and

provide honest answers. Also, the potential of getting all sufficient information through semistructured interviews.

Moreover, generalization will only be limited to the subject or similar event (Zucker, 2009). Yin (2009) and Zucker (2009) recommend continuous evaluation of the data gathered from interviews, observations, and assessments to minimize this risk when extending the findings to other situations. Therefore, narrowing the focus to the evaluation of the effectiveness of technology in combating terrorist organizations' propaganda and networking activities in the cyberspace ensured that the broadness of the topic was avoided. Also, my focus was on Nigeria, which may not apply to another country outside the region. The variations in infrastructure, nature of the economy, politics, and domestic laws will require strategic recommendations to be adjusted when bringing another nation outside West Africa into scope.

Provided sufficient time and adequate resources, another qualitative study approach may mitigate the limitations. Also, scientific research would promote transferability and data validity by comparing different methods in a multiple environment, and the study design provides a methodology to conduct further research. Divergent situations may require alternate governance strategies, and those distinctions may be determined with an analysis of studies. The findings of the study are not absolute. However, the study, though limited in scope, contributed to the social science discipline by highlighting an essential event in the continuum of research.

Significance

This research filled a knowledge gap related to the selection of cybersecurity technologies and their effectiveness and practicality in fighting the expansion of terrorism in Nigeria cyberspace. The 21st-century jihadists have sophisticated and efficient communication strategies (Liang, 2015). Many stories of cybercrime, espionage, and other illicit Internet activity frequently make the headlines of major newspapers in Nigeria. Violent extremists like Boko Haram and ISIS meet openly on social media. Also, they hold private conversations using encryption technology to prevent stranger intrusions. Preventing terrorist propaganda through government sponsored counter-narratives, especially in Nigeria, is largely inadequate and poses a significant challenge for governance in Nigeria (Gourley, 2012, p. 4). The use of information operation (IO) is one of the fundamental pillars of asymmetric warfare (O'Brien, 2003, p. 184), which terrorist organizations are using effectively. Nigeria is only one of many nations where terrorist organizations are taking advantage of the Information Revolution, which has affected the international security agenda and the patterns of the threat actor in the present age (p. 187). The cyber threat landscape is always changing with cyber threat actors increasing the speed and sophistication of their attacks.

The importance of this project is that it touches on an area where there has been limited study, particularly on international best practices and how security administrators make their choice out of the multiple cybersecurity technologies to prevent extremist ideology in a Global South nation such as Nigeria. Terrorist organizations, especially Boko Haram have embraced cyberspace as part of their warfare toolkit, using Nigerian

cyberspace for spreading radical religious ideology, recruiting members, and inciting the public against the government. They use cyberspace to plan and execute attacks. In fact, not fewer than 43 million people in Nigeria have access to the Internet via mobile phones and other technological devices (Musa, 2012, p.116). This represents a significant Internet penetration in the country. There is no doubting the fact that Boko Haram uses new media and mobile phones to spread its message and coordinate all its activities.

Moreover, Nigeria is a representative of the typical global South nation in Africa. The former British colony uses the common law legal system, a federal system of government like the United States, and is a member of the British Commonwealth (CIA, 2017). Nigeria is the most populous black nation with approximately 186 million people (CNN, 2017). The country is an emerging economy in the region with a significant dependence on crude oil and agriculture.

The findings of this study and identified international best practices would potentially be applicable across other nations in West African because of legal and economic similarities. Focusing on its technology sector with 28.4% Internet penetration, the country has sufficiently diverse governmental and commercial systems to make cybersecurity an issue. Furthermore, with the recent upsurge in terrorist activities by groups like Boko Haram, cyberterrorism is a threat to the country's national security (Osho & Onoja, 2015).

Meanwhile, one of the key components of cybersecurity technologies is artificial intelligence (AI). Cybersecurity technologies can help deter/prevent, detect, and defend the cyberspace. The task of mitigating terrorist propaganda in the cyberspace can be

automated through machine learning and artificial intelligence. In a cybersecurity milieu, AI is software that perceives its environment well enough to identify events and take action against a predefined purpose. AI is capable of accomplishing tasks similar to human problem-solving capabilities, using computer algorithms to do things that would typically need human intelligence—such as speech recognition, visual perception, and decision-making. The findings of this study expanded the opportunity to understand how cybersecurity technologies could be used to reduce the effect of terrorist propaganda in the cyberspace. The product of this study and application of suitable techniques will deny the terrorists the anonymity they enjoy in the cyberspace. The social implications of my study are that the Internet will be safer and the social media platform will be free from messages of fear and violence, thereby creating peace and stability, and promoting good governance. It will create confidence for investors and international partners. The result of this study could improve the capacity of the nation to confront a series of threats to its security and simultaneously position itself better to reap the rewards of an Internet-enabled economy. The result of the study provided much-needed insights into the kind of technologies a government can adopt and deploy to neutralize terrorist threats in cyberspace based on acceptable international best practices. Hence, the knowledge of the threats would help the policymaker and researchers to know how to counter it and create a balance between security and civil liberty.

Summary

The Nigerian government is increasingly concerned about the level at which terrorist organizations have embraced technology as an alternative method of

communication and a tool for spreading radical religious ideology, misinformation, and racially and politically motivated messages. Jihadists' strategic use of social media has garnered considerable attention because of its negative social impact. Terrorists gain popularity among their potential supporters by manipulating the public through messages of fear and uncertainty. Meanwhile, terror organizations need social media technology as a logical channel where they can release misleading information such as audio, videos and images to intimidate the public and coerce the government to accept their particular agenda. Meanwhile, confidentiality and secrecy are necessary tactics for the survival of these groups, and that is why they use encrypted communication to evade detection. Researchers have casually mentioned that technology could be a potential countermeasure to mitigate the effects of terrorist misinformation in cyberspace. In my study, I focused on the efficacy of cybersecurity technologies in fighting the expansion and coordination of terrorism in Nigeria cyberspace. The study findings and conclusions empower security planners with new knowledge to defeat cyberterrorists in cyberspace and protect vulnerable populations. In Chapter 2, I focus on the review of relevant literature, whereas in Chapter 3 elaborates on study design, participants, procedures, assessments used, and how I gathered and evaluation the information.

Chapter 2: Literature Review

Introduction

Cyberspace and social media technologies provide advantages over physical media because they offer users the opportunity to operate remotely and remain anonymous as much as possible. This action always involves the use of computer hardware, the Internet, and social media technologies such as Twitter, Facebook, Telegram, YouTube, Chatroom, and Instagram, among others. The capacity to obtain, store, manipulate, communicate and disseminate information through any means available is vital for terror organizations. In cyberspace, terrorists do not need to carry physical weapons, including explosives. However, this locus affords them the opportunity to weaponize information to create crowd psychological effects that stimulate opinions, affect emotions and generate reactions. Technology makes it possible for a small handheld device to generate information from a vast network of global dimensions within a second. Therefore, the availability of the technology and easy access makes it possible for a semi-skilled individual to use a low-cost toolkit to broadcast false information across the world.

Cyberspace technology has enabled a small group of people to create massive disruptions capable of gaining an enormous publicity as physical attacks. A small group of technically skilled cyber terrorists can combine their skills to launch a well-coordinated information operation against the public. For instance, the Aum Shinrikyo terror group in Japan has developed software capabilities to do several things ranging from espionage, to propaganda and malware attacks (Denning, 2000).

Researchers have conducted several studies, documenting counter measures against terrorists' use of cyberspace for misinformation, networking, and coordination. To date, minimal attention has been given to evaluating the effectiveness of technology among other existing possibilities to lessen the social effects of terrorist propaganda and networking in cyberspace.

Hence, a review of research strategies will assist in locating articles that can serve as future reference. The bulk of the discussion will highlight the seminal research, current literature related to the threats of cyberterrorism and various paradigms of cybersecurity strategy, including national security, public health, and economic models.

Literature Search Strategy

The initial search on Google Scholar, using the combination of terms *terrorist propaganda AND social media* returned 143,00 hits. Also, the terms *terrorist propaganda* AND *technology* produced 59,100 results. Further, the terms *terrorist propaganda and technology* returned twelve hits, using Academic Search Premier. The terms *cybersecurity and terrorism* produced 17,400 hits in Google Scholar; Academic Search Premier returned only one hit, although the addition of *developing nations* to the terms resulted to zero. With these terms, other search words such as *terrorism*, *technology*, *cybersecurity*, and *cyber intelligence* were used to narrow down the search. While sifting through the results, it became apparent that there was a gap in research directly focusing on the evaluation of effective technology to combat terrorist campaigns online, especially in the developing or emerging economies such as Nigeria.

The Walden online library produced many of the needed articles for this review. Meanwhile, the cross-cutting nature of cybersecurity made it necessary to look for additional databases. The Homeland Security Digital Library (HSDL), ProQuest Dissertation, and Thesis Database produced multiple sources relevant to the topic.

Given the emerging nature of the field of cybersecurity, new literature search techniques were used within Google Scholar and the Homeland Security Digital Library Database. The terms *terrorist+propaganda+technology+cybersecurity* proved useful in locating newly published sources.

Furthermore, an additional method was the crowdsourcing of emerging materials through participation in a cybersecurity community of interest at the Naval Postgraduate School Center for Homeland Defense and Security. The effort yielded an invaluable result with a diverse network of cybersecurity professionals who routinely discuss current developments and research in the field.

Theoretical Framework

The role of criminology theory such as Cohen and Felson's (1979) RAT in cybersecurity remains open for discussion. The applicability of traditional criminological theory to the study of cyber-related crimes is still in contention in the scholarly community. Several scholars advocate for the development of new criminology theories because the cyberspace environment is a new challenge to criminologists and represents new criminality (Pease 2001; Yar 2005; Reyns et al. 2011). However, Grabosky (2001) posits that the underlying mechanism of criminality in cyberspace is the same as for real-world crimes. The motivation of computer criminals is not new in the sense that they are

driven by greed, lust, power, revenge, and adventure (Grabosky, 2001). Moreover, Foley (2009) argued that routine activity is a resource that has been mostly untapped by students of counterterrorism.

Routine activities of everyday life present opportunities for crime to occur. Cohen & Felson (1979) found that most criminal acts require convergence in space and time, which implies that circumstances must be right for criminal activities to take place. For my study, the argument was be based on the structural changes in routine activity patterns that can influence the rate of terrorist activities in cyberspace by altering the convergence in range and time of the three minimal elements of direct contact predatory violations. RAT requires three situations to be right and happen in space in order for criminal activities to transpire. These are motivated offenders, proper targets, and the absence of protectors against violations. Most crime prevention practice is based on an actor's choice. RAT draws on the rational exploitation of "opportunity: in the context of the regularity of human behavior to design prevention strategies. Therefore, it assumes that criminals are reasonable when there is a capability to operate in the context of attractive high-value targets with weak protection.

In this case, motivated offenders are those who tend to commit all kinds of atrocities for various reasons while the protector is the capability of individuals or organizations to deter motivated offenders such as terrorists from gaining access to cyberspace to commit crime. The opportunity is cyberspace, which serves as a tool for crime and offers protection for offenders. Hence, the security planner may understand and take into cognizance the three tendencies, which are: motivation to commit a crime,

the presence of opportunities and the absence of capable guardianship to prevent crime. Success in the mitigation of terrorist activities in cyberspace will depend upon how best a guardian can deny terrorists access to the "opportunity."

Moreover, Cohen and Felson (1979) developed the RAT to study the rise in crime rates of the 1960s to 1970s, notwithstanding the rapid improvement in living conditions in the United States of America during this period. Cohen and Felson (1979) found that the increase in crime rates in the 1960s was based on the fact that there was an irregular increase in criminal opportunities. It was due to changes in social life after the World War II when women joined the workforce which made them spend more time away from home leaving nobody in the house.

In a similar vein, the change in social life reduces social guardianship because of how the Internet revolution has influenced peoples' way of life in such a way that most people spend more time online, surfing net and conduct transactions in the cyberspace. Hence, it increases the public exposure to violent messages based on the accessibility and visibility of offenders because terrorists have more opportunities to get their messages across to their unprotected targets. Although RAT was formerly used to predict street crime rates, it has been adapted to fit into the study of cybercriminality. Therefore, the choice of RAT for this study is relevant and appropriate because criminal opportunities, such as social media platforms are readily available for cyberterrorists. Therefore, the answer to an upsurge in the rate at which terrorist organizations operate in cyberspace should be sought in the situational structure within which crimes occur. The research question is directly related to the three conditions of RAT. The central research question

is: How do experts see the effectiveness and practicality of cybersecurity technologies as the useful tool to mitigate terrorist networking in cyberspace based on their work experience? The question will provide an answer to the willingness of a nation to apply anti-cybercrime tools and the kind of practical effects on cybercrime at the national level. Also, considering the issue of privacy and civil liberties, the research question will address the practicality of the application of those cybersecurity technologies without violating civil rights and best international practice.

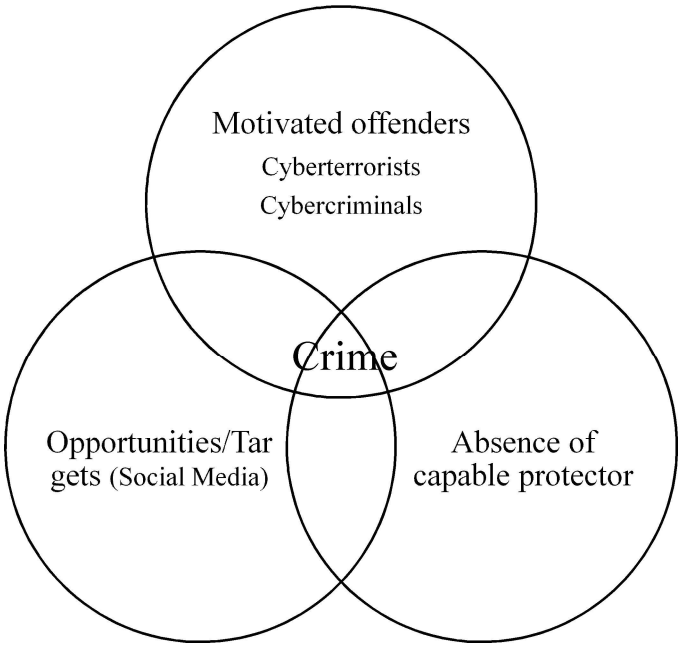

Figure 1. Application of routine activity theory.

RAT provides a theoretical lens which can aid the understanding of the commission of a crime by focusing on the way that daily routine activities affect capable protectorship and target suitability. For instance, computers have become a central part of

everyday life in the past three decades, which allows individual connections with friends and families across infinite distances. More than 25% of Nigerians have access to the Internet (CIA, 2016). Majority of the people can access information from their social media-enabled smartphones, creating a predictable pattern that brings them closer to motivated offenders.

Bossler and Holt (2009) found that RAT has a significant success in explaining a wide range of criminalities such as robbery, burglary, and larceny. Moreover, several scholars have deliberated on how RAT could be applied to cybercrime (Choo, 2011; Kigerl, 2012; Reyns et al., 2011; Stockman, 2014). However, the applicability of RAT to aspects of cyberterrorism, such as the spread of vicious ideology, false information, and recruitment in cyberspace is unclear.

Wall (2001) described the four-fold typology of cybercrime for proper understanding and analysis of the phenomenon. These are cybertrespass, cyber deception/theft, cyberporn/obscenity, and cyberviolence (Holt & Bossler, 2014). Cyber violence is divided into two: an examination of the networks of hate speech of extremist groups, and cyberterrorism. Experts agree that the issue of hate speech and extremist groups has been examined extensively compared to cyberterrorism that has been under research (Holt & Bossler 2014; Brenner 2007).

Although all are perpetrated with the use of computers in cyberspace, there is a definitional difference between cybercrime and cyberterrorism (Che, 2007). Whereas cybercrimes are crimes where the perpetrator uses special knowledge of cyberspace, cyberterrorism is the use of computer network tools to attack critical infrastructures or to

coerce or intimidate governments and civilian populations (Che, 2007; Denning, 2000; Lewis, 2002; Martin & Weinberg, 2016).

The literature review identified seven studies that have used RAT to explain cybercrimes, especially victimization in cybercrimes. All these studies provided different outcomes as related to the usability of RAT because the studies focus on various cybercrimes and utilized RAT aspects in different ways. For instance, Choi (2008) found that technical guardianship has the potential of decreasing risk of victimization in the cyber environment. The study applied RAT to examine on-line activities such as using email and downloading, and technical guardianship such as anti-malware software.

Holt and Bossler (2009) examined the effect of routine computer usage and concluded that the RAT does not affect the chances of online harassment. However, the time spent in chat rooms and involvement in computer deviance increases the risk. Holt and Bossler (2009) established the fact that exposure to other people in the cyberspace environment does not increase the chances of victimization but spending time online with others in particular contexts increase the risk.

Also, Marcum et al. (2010) applied RAT to study three kinds of online victimization and concluded that engaging in behavior that increased exposure to motivated offenders target suitability promote the likelihood of three types of victimization measured. This study implies that protective measures such as capable guardianship may not reduce the prospect of victimization.

Furthermore, Reyns, Henson, and Fisher (2011) used RAT to assess cyberstalking victimization by looking at the effect of online visibility, accessibility, and guardianship.

The quantitative study showed that variables did not produce consistent results across the types of pursuit behaviors. Part of the conclusions is that adding strangers on social media platforms is significantly related to victimization.

In summary, RAT will be the theoretical framework for the proposed study: Countering Terrorists' Propaganda: Experts Evaluation of Effectiveness of Cybersecurity Technologies. RAT is a useful analytical tool to determine the underlying mechanisms that cause crime. Empirical research has established that RAT can successfully predict crime and victimization across a plethora of crime typologies. The proposed study intends to provide an answer to how experts see the effectiveness of technology in mitigating terrorist propaganda and networking in cyberspace based on their work experience.

Literature Review Related to Key Concepts

In this section of Chapter 2, the literature on terrorism will be reviewed to understand the concept of cyberterrorism with a focus on online terrorist propaganda and how terrorist organizations have been using cyberspace to propagate violent ideology. The review will include how social media platforms have become veritable tools in the hands of terrorists. The study will look into the difference between cybercrime and cyberterrorism and how terrorist organizations are engaging in both activities. Furthermore, the study will review a national security approach to cyberterrorism.

In fighting terrorism, it is important to understand the fact that the presence and nature of the threat change daily. The next war will be in cyberspace and terror organizations pose a significant threat to global security. Hence, the emerging threat is

cyberterrorism. Of course, the U.S. and the world have put proper emphasis on this potential growing threat in the war on terror. Cordesman and Cordesman (2002) suggested that the National Intelligence Council has taken a broader view of these emerging asymmetric and strategic weapon of mass destruction (WMD) threat. The U.S. plans to maintain a high technological edge in the IT-driven "battlefield awareness" (p. 30). The power of terrorist propaganda on the public is enormous to the extent that individuals act because they have been influenced by a message sent through social media technologies. It is disturbing that the terror organizations all over the world have embraced technology to advance their violent agenda. Terrorism is an attack on open societies and terrorists' activities on the web spread messages of violence, hate and panic, posing a significant threat to the world. "Online Jihadism" and "Cyber Jihadists" are emerging threats that require mitigation. The literature review will discuss what constitutes cyberterrorism, including terrorists' use of social media technology, terrorist propaganda (Cyber Jihad), and terrorist communication and networking activities in cyberspace.

Terrorism

The word terrorism is a deliberate creation of fear, violence or the threat of violence, used by its perpetrators in the pursuit of political agendas (Berkebile, 2017; Martin & Weinberg 2016; Sandler, 2015). A terrorist is the perpetrator of the act and those who use terror or terrorism, including individuals of a state or individuals associated with a non-state entity in pursuit of political views by a system of coercive

intimidation, violence or fear. Hence, terrorism is an act of violent coercion to pursue power (Hoffman, 2006; Mahan & Griset, 2013).

Those who are competing for power, for political, ideological or religious change, and dictatorial governments that want to preserve power, have used terror to instill fear in people. Terrorism is not new; it is a phenomenon that has a long history, longer than that of the modern nation-state. Abrahms and Conrad (2017) have argued that terrorism is an instrumental violence that functions as a political communication strategy.

The Global Terrorism Index (2016) indicates that there are 28 terrorist groups in Africa. Some of them are Algeria's Armed Islamic Group, the Lord's Resistance Army in Uganda, Ansar Dine, the Tuareg in Mali, and Al Shabaab in Somalia, which claimed responsibility for the Westgate shopping mall terror attack in Kenya in September 2013. Boko Haram in Nigeria has become the most active terror group in Africa both on the ground and in cyberspace. Boko Haram swore an oath of allegiance to ISIS and the group is currently known as ISIS in West Africa.

Terrorism means different things to different people, and there is no single accepted definition for several political reasons. Several types of research point to the fact that terrorism creates uncertainty in the society, harms and kills innocent people, and destroys properties (Allision, Anne & Ahmet, 2017; Berkebile, 2017; Hoffman, 2016; Martin & Weinberg 2016; Sandler, 2015). Despite the lack of universal definition, parallels can be found among each description: violent acts, unjustified by law, with sociopolitical objectives. Hence, reducing terrorist attacks by taking attack weapons away from them is a worthy goal.

Terrorist Propaganda

One of the essential terror instruments is media propaganda; there is no doubt that any terrorist operation without the media has limited effects on the targeted audience. The invention of social media technology, which enables terrorists to bypass middlemen before reaching their audience is an added advantage for such groups. One significant objective of terror groups is to get maximum publicity for their terrorist activities. Instead, the devastating effect would be restricted to the immediate victims of their dastardly deeds. Hoffman (2006) pointed to the fact that terrorism and media are joined together in an intrinsically symbiotic relationship, each feeding off and utilizing the other for its purposes (p. 183). The terrorist always wants to communicate the revolutionary or divine messages to a broad audience, and the group has recognized the potential of new mass communication technology.

The Internet and the media technology through social media platforms has been a useful tool for terrorist organizations. The power of images blended with text can cause panic and influence public opinion on major issues. Pictures of violence have a reasonable influence on the public and the policy maker and thereby affect both domestic and foreign policies. ISIS remains the most potent terrorist organization in modern history, possessing sophisticated cyber capability. ISIS recruits young jihadists using over 21 languages over the Internet. The group is using YouTube videos, memes, tweets and other social media postings and flooding cyberspace for their sympathizers to retweet, like, or endorse their materials to recruit members into their folds (Allision, Anne & Ahmet, 2017; Hoffman, 2016; Kaplan & Malkki, 2014). Also, Weeraratne (2017)

uncovered that ISIS partnered with other terrorist groups like Boko Haram to spread its messages and provided cyber and media training to them. Through this partnership, Boko Haram was exposed to and subsequently developed new tactics, and was provided with symbiotic relationships with other groups through which the Boko Haram message could be propagated. The mutual relationship between the two group granted Boko Haram unfettered access to Al Qaeda's Al-Andalus media arm, which assists in the area of the propaganda campaign.

In the present media age, terror organizations have discovered social media technology as an extra and vital weapon in the sustenance of their struggle. In the past, particularly during the Cold War era, terrorist organizations could only depend on three primary communication techniques: secret rebel radio stations, clandestine publications such as posters and handbills, and traditional public media agencies, including state-owned mass media. However, the new media age has afforded terror organizations further opportunities to control their self-media propaganda machines.

Hoffman (2016) proposed counterterrorism measures such as denial of the enemy, cyber sanctuary, and the elimination of terrorist resources that enable the group to conduct cyber mobilization and recruitment. Moreover, the creation of a secure environment, including comprehensive and integrated information operation (IO) are critical factors to consider for counterterrorism operations.

Understanding Cyberterrorism

Cyberterrorism refers to a computer-aided terror act. The term is a combination of cyberspace and terrorism. Cyberterrorism is a politically motivated attack that generates

fear or harm. It should result in violence or threat of violence against persons or properties. Murril (2011) posited that the term could be misleading, and the response could be based on who is defining it. “Cyberterrorism” means various things to different people, depending on the actors, which may result in different responses. Cyber terrorists are cyber actors or groups with a direct or indirect association with a formally recognized terrorist group. They often use a threat of violence to instill fear in general populations or victims in order for the targets to comply with their demands or ideology. Their action in cyberspace can be termed cyberterrorism and may result in counterterrorism responses. Transnational terrorists use online tactics like “cyber-mobilization”, and computer malware as economic weapons (Martin & Weinberg, 2016). Terror groups around the world, including Boko Haram in Nigeria, use technology to spread violent ideology and recruit members.

Meanwhile, a lone individual whose motivation is personal or financial gain that uses malware and sophisticated tactics against intended targets will get a different response. The lone individual who commits crime for personal financial gain may be regarded as a cybercriminal. Also, hacktivists are different from cyberterrorists in another aspect. Hacktivism is a blend of hacking and activism; it is the subversive use of computers and networks for a political and personal purpose. The threat is lower compared with cyberterrorism because the purpose is to draw the attention of target governments to an ideological cause such as free speech, human rights, and environmental concerns.

Early research asserted that the use of the Internet to communicate, coordinate events and actions does not necessarily constitute cyberterrorism (Che, 2007; Denning, 2000). Che (2007) points out that cyberterrorism is hard to define—just like terrorism; however,-a cyber hacktivist is different from a terrorist who uses technology to propagate radical ideology, hate, and violence. The study posited that technological intervention such as surveillance and censorship in the age of terrorism might have a legal implication. On the contrary, a prior research recommended that a strict regulation that requires Information Service Providers (ISPs) to collect and confirm valid information about their subscribers may deter or discourage terrorist communication (Hinnen, 2004).

Nevertheless, Al Mazari et al. (2016) developed cyberterrorism taxonomies to include cyber-attacks against social and national identity. Their study observed a number of acts that were deemed cyberterrorism. These included the defacement of government and organization websites, the spread of false rumors, violence, hate messages, and misrepresentation against a social target and entities, using social media technologies.

Meanwhile, the literature often uses the term cyberterrorism to describe terrorists' online activities, including communication and spread of propaganda (Rogan, 2006). Moreover, Martin and Weinberg (2015) bridged the gap between academic thought on the areas of terrorism and mass political violence, taking time to explore and develop accepted definitions of many terms in the field. The study suggests that terrorist organizations engage in cyber-mobilization and the use of computer malware as economic weapons. The study proposes that the method to stop cyberterrorists should

encompass non-state and non-military actors and the need in which academic thought and theory can catch up to the realities of modern-day warfare.

However, Goodman (2007) suggested that the concerns should be about what terrorist organizations will most likely do in cyberspace, which is to support their activities and infrastructure, and one of those activities is propaganda. Terrorist organizations use cyberspace for several things, including the spread of their ideology, promotion of violence, indoctrination of adherents, recruitment of members, perpetration of crimes, and misrepresentation to cause fear and panic (Conway, 2002; Hinnen, 2004; Ki-moon 2012; Ogun, 2012; Weimann 2006).

Benson (2014) has a different theme as the study argues that as terrorists have increased their use of the Internet, state security organs have far outpaced them, leading to a much less dramatic rise in cyberterrorism than is currently thought. The study suggests that a significant amount of terrorist activity is fundamentally a local endeavor and that local initiatives do not benefit from better access to transnational communications devices. As for transnational terrorism, such non-local or non-regional initiatives inherently draw support from a non-local base, and could therefore better benefit from a transnational support system buoyed by a transnational (and often anonymous) communications system. It has been consistently assumed in the standard literature that the Internet facilitates transnational terrorism—in particular with the influence of anonymity, abundance of information, and the inexpensive nature of online communications.

Minei and Matusitz (2011) share similar thoughts and have discovered that such communications networks and social media allow groups to form, and the spread of vital information tolerates individuals (lone wolves) who are influenced by the terrorist messages to take action and attack their homeland. Meanwhile, referring to Hair and Health (2005), researchers agreed and aligned with the previous sentiment that cyberterrorism remains a communicative process because both intentional and clandestine communications between cyberterrorists and their targets occur through different modes of propaganda (Conway, 2002; Weimann, 2006). For instance, ISIS supporters used social media to call on their fellow terrorists to poison food in grocery stores across Europe and the United States of America (Moor, 2017). The group posted the graphic message through the encrypted messaging application Telegram, a platform favored by cyber jihadists to disseminate information to members while maintaining secrecy and privacy.

Benson (2014) suggests that in the same way, governments can also disseminate information in support of their interests. Anonymity, thought to be a benefit to terrorists, can also serve to mask surveillance efforts and facilitate counter-surveillance. This study suggests that Internet anonymity is incorrectly assumed and that state-based organizations have ample resources to push through this assumed anonymity, monitor groups, and set up sting operations to catch users. Furthermore, the increased information available to terrorists may not be accurate, may lack filters, and may lead to an inability to make clear decisions. The research posits that just because a person has access to cookbooks does not make them a master chef able to put a gourmet dinner on the table. In the same way,

access to terroristic information does not make a person a terrorist or bring destructive acts to the national stage. Benson (2014) asserted that Al Qaeda was dangerous and more powerful before the Internet. The study suggests that homegrown terrorism, and an analysis of Al Qaeda in pre- and post-Internet periods gave a clear idea of how terrorists might use cyberspace to their advantage as additional weapons. The study determines that the Internet is a tool for civilization rather than chaos, and extends that idea to various local situations in Africa in which access to cyber resources did not coincide with an increase in terrorist actions.

Terrorists' use of Social Media Technology

It appears that terrorists are shifting to cyberspace with every device becoming a battleground with the aid of social media technology. Research suggests that social media technology is the major tool used by terror organizations to recruit new members and spread their propaganda (Berger, 2015; Conway, 2002; Ranger, 2017; Rogan, 2006). In today's world, social media outlets have become part of daily life with terrorists using these media to send messages of fear. How terrorists use social media to perpetrate its agenda points to the future. Lohrmann (2016) found that ISIS has been using the Internet successfully to recruit new fighters through new media technology such as Facebook, Twitter, YouTube, and Telegram. The study suggests that social media technology is the central tool to spread hateful and violent messages. Attention-seeking terrorists have been using social media in new ways to reach out to mass audiences with their message.

Moreover, electronic jihad via strategic messaging and communication has become the manifestation of modern-day terror with the use of online media technologies

to disseminate sophisticated multidimensional information. Liang (2015) discovered that the application of social media technology such as Twitter, Facebook, Instagram, Telegram, Chatroom facilitated communication and coordination at a global level outside of the control of governments. The increased connectivity created challenges that traditional law and international agreements could not easily resolve. Researchers have argued that the Internet frontline needs a proactive defense because censorship and the removal of terrorist content is reactive and not effective.

Furthermore, in a research paper presented by former FBI Director of Intelligence and Counterintelligence at the13th Annual Conference of the International Association for Intelligence Education, the study examined why terrorists choose social media platforms. The research found that terrorists prefer this dynamic because it is hard to stop the spread of online misinformation (D. Major, keynote speech, May 23, 2017).

Also, a report titled "The evolution of terrorist propaganda: The Paris attack and social media" by the United States House Committee on Foreign Affairs' Subcommittee on Terrorism, Nonproliferation and Trade questioned why social media companies would allow terrorist content on their platforms. The report found that Twitter remains the favorite and most widely used platform by terror organizations while Facebook has become the terrorist favorite platform to share photos on message boards (Berger, 2015). The report claimed that among social media companies, Twitter is far worse than the rest with regard to acting proactively to track and remove terrorist content. The committee's report discovered that the ISIS is using new technology to escape detection and the eventual removal of its content when posted on YouTube. The ISIS uses a service known

as “Vimeo” to post graphic violence. YouTube tried but did not succeed in removing them all. Among the counter radicalization strategies that the White House published in 2011 was the commitment to devise means to deal with the new threat, including the use of intelligence led strategy which consist of right resources, tools, and process to defend against cyberterrorism (Berger, 2015). What is not known is how the technology will be deployed and how effective it will be. Meanwhile, a coalition of top technology companies in the United States is making efforts to curb terrorists’ use of social media technology with the use of Artificial Intelligence (AI). Korolov (2017 explained that AI-based security applications can read and understand security — they can analyze every incident, identify causes, methods, trends and predict the next pattern even before it happens. For instance, IBM developed Watson, which has been taught to read through vast quantities of information online (Lee, 2015). Watson provides smart data analysis and visualization services, which makes it easy to detect patterns. It has an inbuilt capability that enables the user to interact with data in a conversation with a response the user can easily understand. In some countries of Global North, the Law Enforcement and intelligence agencies are using AI, and machine learning to detect and respond to different kinds of cyber threats, including cyberterrorism. There are different kinds of cybersecurity tools available, but the user or organizations must know how to apply them and integrate them into the broader cybersecurity strategy. Isaac (2016) found that there is an ongoing project to create a shared digital database which includes “fingerprinting” or patterns of all suspicious terrorist content that raise red flags. This inter-company

collaboration will ensure that content that has been flagged on Twitter will not appear on Facebook or another social media platform.

Another aspect that creates challenges is the capability of cyberterrorists to remain elusive while perpetrating their act. Schultz (2015) argues that the ability to operate undetected while using online tactics makes terror groups real beneficiaries of cyberspace technology. Terrorist enjoys the anonymity the cyberspace provides them. Stealth is the most significant advantage of the Internet. Kaplan (2009) pointed out that terrorists swim in the ocean of bits and bytes, which make it difficult to identify the real culprits or bad actors. The secure means of communication through encryption tools, steganography, dead dropping (transmitting information through saved emails drafts in an online email account to anyone with the password) makes them elusive. The study suggests that the utilization of social media outlets gives terror organizations a global reach, and enables them to mobilize new members and instill loyalty among their followers through constant and clear communication. Terrorists have embraced cybertechnology, which empowers them to decentralize their activities and makes it hard to target them through conventional military capability. Current efforts to diminish online terrorist operations, including the spread of messages of violence are inadequate. The study suggests that there is a need for an innovative strategy to deal with online threats from cyberterrorists. There is no doubt that terrorists are susceptible to deception and failure in cyberspace just like the same protection that the cyber technology offers the group (Schultz, 2015).

In Schultz's study, false-flag operations (FFO) are recommended as one option to tackle terrorists' online activities. FFO is a military deception method originated from naval warfare. The researcher found that FFO could be used to compromise terrorist narratives on social media platforms so that extremist groups will grow to distrust their websites because their ideological messages will be altered to deviate from their approved narratives. What is unknown is how effective FFO could be in mitigating this risk.

Terrorists and Cybercrime

There is a thin line between cybercrime and cyberterrorism as terrorists engage in both activities. Terrorists uses cyberspace to coordinate terrorist activities, which is regarded as cyberterrorism. Terror organizations manipulate the public, spread messages of hate and violence, and recruit members in cyberspace with the aid of social media technologies in furtherance of their agenda. They also inspire individual "lone wolves" to commit acts of terror against their homeland on their volition. Also, terror organizations engage in cybercrime such as identity theft, hacking, extortion, phishing, and money laundry to fund their terrorist operations. Acts of violence against computer networks and the use of the social media technology to perpetrate violence can be regarded as cybercrime. It is important to make the distinction that not all cybercrimes are terrorist crime. It depends on the factors and the intention of the threat actors, which may fall within the definition of cybercrime or cyberterrorism. Holt (2016) corroborated several research arguments that there is no single accepted definition for both cyberterrorism and cybercrime. Holt's study pointed to a framework with four distinct categories of

cybercrimes, which are cyber-pass, breaches of computer networks and system boundaries, cyber deception, and cyber violence. The study found that the problem with defining cyberterrorism lies in distinguishing these acts from cybercrimes. Hence, the interconnectivity enabled by the Internet empowered the attackers to target their audience to create emotional harm or commit crime through identity theft, illegal gambling, money laundering, hacking and cyber exploitation, and the distribution of child pornography. Terrorists are known to engage in the act of expropriation by robbing public institutions like banks, offices, businesses, and citizens to finance terror activities either through physical or virtual means.

Cybercrime is an illegal act which is carried out with the use of computers and computer networks. It involves the interruption of network traffic, denial of services, the creation and distribution of malware, extortion, impersonation, and the distribution of child pornography (Adomi & Igun, 2008). There is a thin line between cybercrime and cyberterrorism which causes the media and researchers to use both terms interchangeably in many instances. Researchers distinguish the two based on actors, motives, and targets. Cybercriminals launch attacks for personal financial gain while cyberterrorists are driven by motives such as political change, ideology, religion, vengeance, or social change.

A cyberterrorist is an actor who launches attacks to intimidate a government or a public in order to advance ideological, political or social, religious objectives. Terror organizations use cyberspace, especially social media technology to prepare, participate in, and coordinate terrorist agendas. Sageman (2008) argued that modern-day jihadists are self-recruited with the support of the Internet where they are able to locate their

comrades on the cyber web. For instance, many of ISIS' foreign fighters were recruited through social media platforms (Foley, 2009). In Nigeria, Boko Haram gained unauthorized access to the Nigeria Secret Police, popularly known as State Security Services (SSS) to obtain vital identities of government officials to target them for terror attacks (Osho & Onoja, 2015).

Although terrorists tend to engage in cybercrimes like identify theft, online fraud, phishing scams, and cyber extortion to raise money to support their operations, cybercriminals differ in that they do not participate in those activities to promote ideological, religious or social change. While cyberterrorists are driven by political or ideological agendas, hacktivists mission are to draw attention for ideological cause or to express opinion though cyber protest or activist agenda. Cybercrime is a crime of opportunity where an individual seeks to gain personal benefit from the proceeds of crimes. Cyberterrorists are disciplined, trained and committed actors who are motivated by ideology, religion or political agendas. Also, nation state can engage in cyberterrorism against another nation through information operation or can participate in cybercrime to steal proprietary information or trade secret from another country.

Terrorist organizations are most likely to use cyber weapons than nation-state actors. The most obvious way that the terrorists have been using cyber technology is for communication and planning. The group discusses in the open, using social media platform and coordinate their secure conversation with the encryption technology. Fink, Pagliery and Segall (2015) pointed out that this method of secretive communication which is known as "going dark" remains one of the significant challenges facing

intelligence community, police and counterterrorism officials all over the world at the moment.

Moreover, one of the most apparent differences between cybercriminals and cyberterrorists is their motives. The primary goal of cybercriminals is to commit a crime of opportunity and stay hidden to enjoy the proceed of their exploit. Terrorists want to spread messages of hate and want their content to go viral to create fear and uncertainty.

Table 1

Difference Between Cyberterrorists and Cybercriminals

Terrorists (Motives and methods)	Criminals (motives and methods)
Ideology, religion political	Financial or personal gain
Psychological warfare	Data mining: identify theft, credit card scam
Publicity, propaganda, and information sharing	Espionage or competitive advantage
Recruitment and training/networking	Fun, curiosity, or pride
Fundraising, money laundering	Grudge or personal offense
Data mining	Money laundering, fraud
Planning and coordination	

In addition, Ndubueze and Igbo (2013) revealed that Nigeria leads the African continent in use of the Internet—both in the percentage of Nigerians with access to the Internet and the percentage that these users represent across Africa as a whole. Therefore, easy access to the Internet enabled terror organizations such as Boko Haram to use social media technology such as YouTube to spread their ideology. Perpetrators can operate from public cybercafés or use private masked IP addresses for some secret operations to evade detection. According to the Ndubueze and Igbo (2013), Nigeria's Advance Fee Fraud and Other Fraud Related Offences Act (2006) mandates that cybercafe managers

are held responsible for online activities carried out in their premises, and maintain a database of customers for this purpose.

National Security Approach to Cyberterrorism

The dominant theme in cybersecurity strategy is national security and understanding the fact that cyberspace is a critical infrastructure that needs to be protected. The essence of this theme is to ensure that all cyber infrastructures are protected from terrorist organizations and cyber criminals (Osho & Onoja, 2015; Schechner, 2015; Schweitzer, 2015; Weimann, 2014).

Harknett, Callaghan, and Kauffman (2010) found that the Internet was designed for the military environment and this idea is consistent in Harknett's work (Harknett et al., 2010; Harknett & Stever, 2009). Hence, the cyber environment is a place where the offensive method dominates the defensive response. Also, it diminishes the role of deterrence and legal strictures on nation states and criminal actors. The arguments also tend to emphasize that the absence of protectors who are competent to defend targets and victims creates an opportunity for willing potential lawbreakers with the capacity to commit crime (Miró, 2014).

Terrorists' use of cyberspace to perpetrate violence and misinformation has implications for national security and most countries are incorporating the plan of action to mitigate the threat into cybersecurity strategy. Osho and Onoja (2015) investigated the content of the Nigerian National Cybersecurity Policy and Strategy drafts of 2014 to evaluate concrete plans and action to combat cyberterrorism and terrorists' use of technology to spread violence and hate messages in the draft. Osho and Onoja (2015)

looks at economic cybercrime and threats to national technology infrastructure, but has useful analytic comparisons of the strategies employed by other countries to combat terrorists' use of technology to perpetrate violence, misinformation, and other crimes. Especially interesting are those of Kenya, the United Kingdom, the Netherlands, and France. Osho and Onoja (2015) compares the Nigerian National Cyber Security Policy and Strategy drafts to five similar international policies, and to the policies of seven industrialized nations. The Osho and Onoja (2015) concluded that the Nigerian National Cyber Security Policy and Strategy drafts are roughly comparable in content to the other policies. However, the study found that the Nigerian National Cyber Security Policy and Strategy drafts are desperately lacking in the following areas: technological infrastructure, the establishment of secure cyberspace and ongoing attention to digital identity frameworks, explanation of the current national cyber security state, ongoing partnerships with Internet providers, and a focus on military-based cyber defense capability.

Researchers have recommended some cyber defense capabilities such as Social Network Analysis (SNA). The SNA makes it possible to map the users of social media technology through their use of instruments such as Internet communication and phone calls. The process has been in widespread use since 9/11 and is a prime means of discovering key agents in terrorist networks (Olajide & Adeshakin, 2016). The application of SNA tools can be used to expose the email addresses of known terrorists and associated Facebook pages. Olajide and Adeshakin (2016) suggest that the use of SNA would probably have disrupted the communication and networking of the 9/11

hijackers. Olajide and Adeshakin's (2016) proposal and recommendations are feasible and could be applied to Nigeria's national security strategy. Hence, (a) SNA should be used in the future, as terrorists make liberal use of phone calls to communicate; and (b) terrorist-related videos posted to social media and other cyber networks can be applied to the same tools to decipher networks and potentially counter violent operations.

It is known that terrorist organizations are using online tactics to spread fear, panic and present situations of uncertainty to the public (Conway, 2002; Dean et al., 2012; Ki-moon 2012; Rogers, 2016; Liang, 2015; Minei & Matusitz, 2011; Ogun, 2012; Ranger, 2017; Weimann, 2014). Social media is an efficient and convenient tool for terrorist groups because it has the capability of spreading short messages with blends of image, voice, and text (Holt, 2016). Every device such as laptop computers, desktop computers, mobile phones, and digital watches have Internet access capability and network to reinforce ideological beliefs and spin messages. Young people have been encouraged via social media to take terrorist action against their homelands. Several examples of the last few years indicate that ISIS mobilized young people via social media to travel and join jihadists in the war in Syria. Most *fatawi* issues by terrorist leaders are communicated to the public via social media.

Also, it is known that measures to counter online terror tactics remain inadequate and there is a need for a strategic solution to combat extremist narratives in cyberspace (Berger, 2015; Dean et al., 2012; Musa, 2012; Olufemi et al., 2013; Schultz, 2015). We know from the literature review that the cyberterrorists motivation is to instill fear so that targets will comply with their demands and ideology. The terrorist organizations are

currently using cyber technologies to advance their programs such as recruiting, inciting, training, planning and financial gain. There is a growing fear that terrorists can quickly acquire destructive capabilities. It is a known fact that the Internet provides unique opportunities to commit a crime and the terrorist organizations are using the opportunity to engage in information operation to terrorize the public with the message of fear, violence and radical ideology. It is also known that the Internet has become a routine activity in everyday life, which create an opportunity for the cyberterrorists to target their victims with their messages. It is established from various studies that lack of guardianship both technical and legislative instruments may be part of the reasons for the rise in terrorist organizations uses of the social media to generate violent ideology and spread propaganda (Choi, 2008; Koops, 2010).

What is not known, however, is how security experts and security administrators make their selection of cybersecurity technologies that best fit the status of technical guardianship in the cyberspace. Also, their perception of effectiveness and practicability in term of the kind of technology that has been most useful to stop terrorist networking in cyberspace. RAT may provide insights on how cyberspace can be best protected by excluding one of the three elements from the equation. Terrorists and cybercriminals are currently using social media technology to their advantage. Hence, there is a need to devise an adequate strategy that removes the protection that cyberspace offers to cyberterrorists.

Summary and Conclusions

The literature on cyberterrorism continues to emerge, but there is a consensus on the need for a comprehensive strategy to limit risk and better secure cyberspace from the threat of cyber terrorists (Cordesman & Cordesman, 2002; Isaac, 2016; Lohrmann, 2016; Schultz, 2015). The threat landscape is evolving with the advent of social media technology, which provides a platform for actors to mobilize, communicate and recruit members. Moreover, the ideology that the group spreads on the Internet breeds violence, and creates panic and uncertainty in societies. Kaplan (2009) explained that defining cyberterrorism or terrorist website is as contentious as defining terrorism. While Cyberterrorism is the use of the Internet as a vehicle through which to launch an attack, the supporters, sympathizers and web couriers of terror activities are all terrorists.

The applicability of criminology theories, such as RAT is proposed for the study because all the underlying mechanisms of criminality in cyberspace are similar to real-world situations. Some scholars differ though, claiming that there is a need to develop new theories that apply to the cyberspace environment. Meanwhile, RAT will provide a theoretical lens to understand how crime is committed when the circumstances are right. In the context of cyberterrorism, an assumption is that cyberterrorists are criminal politically motivated actors that seek opportunities afforded by cyberspace anonymity without geographical limitations, develop a necessary capability for cybercrime, and target weakly protected systems (Broadhurst & Choo, 2011).

Terrorism is a global phenomenon, and terrorist organizations are embracing technology to spread their ideology. Terrorism is “premeditated, politically motivated

violence perpetrated against noncombatant targets by sub-national groups or clandestine agents" (CIA, 2016). It is important to understand that terrorism has been in existence for centuries, and is getting more sophisticated with advances in technology. There is no "magic bullet", there are no perfect solutions, and there will never be a clean victory.

The vital instrument of terrorist organizations is media propaganda because their intention is to derive maximum publicity from their actions. Hence, cyberspace remains an essential tool for their ideological propagation, recruitment, and communication. It is no easier to define cyberterrorism than it is to arrive at a single accepted definition of terrorism. Nigeria regards terrorism as a crime like Britain and France (Foley, 2009). It is a legal offense to participate in, prepare or propagate terrorist activity (Foley, 2009).

Experts agree that social media technology is a significant tool for terrorist organizations, including Boko Haram in Nigeria. How terrorists use social media is a signpost for the future. Therefore, the proposed study will be the best fit on how to foster the culture of security and the need for active guardianship with the application of technology. The study will answer questions about the kind of technology that has been most useful for mitigating terrorist networking in cyberspace from the perspectives of experts' professional experiences

Chapter 3: Research Method

Introduction

The current global trend points to the fact that terrorists will continue to use cyberspace, including encryption technology and dark web, for recruitment and to spread propaganda. Also, they will use the cyberspace to encourage lone-wolf actors and facilitate operation with the ability to conduct physical attacks against the targets (NJCCIC, 2018). This study was a qualitative interview structured to explore the perception of security experts on the role of technology in attacking terrorism in Nigeria cyberspace. Also, I probed into how experts make their choice of cybersecurity technologies, including its effectiveness and its practicality in mitigating terrorist propaganda and expansion of terrorism in Nigeria cyberspace.

Research Design and Rationale

This study was aimed to answer two research questions, following a logical order based upon the findings for the previous one. They were:

1. How do the experts see the role of technology in fighting expansion and organization of terrorism in cyberspace?
2. How do experts perceive the effectiveness and practicality of cybersecurity technologies as a tool to mitigate terrorist propaganda and networking in cyberspace?

Terrorism in cyberspace was the central phenomenon that I addressed in this study, and I focused on cybersecurity technologies capable of fighting the organization of

terrorism in the cyberspace. I based my assessments on the opinions of the selected security experts.

This qualitative study was guided by Cohen and Felson's (1979) RAT as the theoretical framework. As an environmental, place-based account, the theory argues that three elements must converge for a crime to occur. Miró (2014) argued that the absence of protection creates an opportunity for a potential criminal that has the means to commit a crime. The data collected was continually interpreted in light of the problems and issue arising in the context of the study. This process was used to understand how terrorists make their decisions to use cyberspace for terror activities and how the choice of suitable cybersecurity technologies could frustrate them and decrease their motivation.

Research Question 1 was aimed to assess the current thoughts on terrorism, cyberterrorism, including cyberterrorists and the role of technologies in fighting the menace in the cyberspace. I obtained answers to establish standard themes as the basis for recommendations in the context of Nigeria. Also, I used Research Question 2 to frame the recommendations related to the choice of cybersecurity technologies and the context at which the selected tools would be efficient and practical to use without any violations or raise civil liberties concern.

A qualitative research interviewing design was appropriate for exploring the phenomenon being studied by investigating professionals' views. Boyce and Neale (2006) explained that in-depth interviews are appropriate when a researcher intends to discover new issues and get detailed information about a person's thought and behavior.

Qualitative research interviews design matches the qualitative methodology and critical theory interpretive analysis. Moreover, qualitative research interviews design gives realistic inquiry of the multifaceted phenomenon with accuracy. The goal of an interview is to find a description of the life-world of the interviewee as related to the interpretation of the meanings of the described phenomena (Alshenqeeti, 2014; Turner III, 2010). The researcher will be able to talk to those who have a clear understanding of the issue of interest and explore in detail the motives and opinion of others to learn from their perspectives (Boyce & Neale, 2006; Rubin & Rubin, 2012). Therefore, the study gained insight into how experts perceive the role of technologies in fighting the expansion of terrorism in cyberspace, including the effectiveness and practicality of offensive cyber technology based on their work experiences. Through this qualitative interview study, the experts sought to identify the threat and how to manage the risks from strategic, operational and tactical levels. Also, the investigation revealed needed improvement for the Nigeria government, including response readiness.

Rationale for Qualitative Interviews

The choice of intensive interviewing is appropriate when there is a need to understand the ideas and motivations for people's action, or how they operate in particular situations (Boyce & Neale, 2006; Rubin & Rubin, 2012; Turner III,2010). It enables a researcher to connect directly with the population and community of concern. The study used a semi-structured open-ended interview approach. Turner III (2010) identified three forms of interviews, which are a formal conversational interview, general interview guide approach, and standardized open-ended interview. A researcher can use

any of these formats to obtain rich data based on qualitative investigational perspectives. Qualitative assessment via interview can get at certain underlying realities of the situation because it allows more in-depth examination of the issues (Creswell, 2009). Qualitative assessment methods through a semistructured interview enabled the study to collect information directly from security and intelligence community members themselves. It allowed experts to fill in the details as much as they can on their perception about the effectiveness of cybersecurity technologies and the reason for their choice. Meanwhile, being interviewed is more likely to leave participants feeling like part of the process than filling out a survey. Rubin & Rubin (2012) explained that qualitative Interviewing is beyond the idea of collecting data but it a form of seeing the world and learning from it. Also, qualitative research interviews have been the basis for many studies across different disciplinary fields, including social sciences and Homeland Security studies (Edwards & Holland, 2013; Rubin & Rubin, 2012).

Pelfrey (2009) used qualitative research interviews to assess homeland security preparedness by conducting interviews with those agency administrators tasked with coordinating terrorism prevention. The research discovered that most officers had not received enough, or no training as regards to terrorism prevention.

Moreover, interview of key players from security and public sectors is paramount to obtaining the perception of how they evaluate the effectiveness of current technologies. Qualitative research interviews make security professionals, including law enforcement agents more understandable to the consumers of their products. There are security professionals in different agencies and with a different focus; counterterrorism;

security professionals with various institutional affiliations, educations and experience backgrounds; and lawmakers, public officials, personnel and cybersecurity advisors with distinctive functions and depths of understanding of the cybersecurity technologies.

Security planners need to understand when, how, and why people end up using or not using cybersecurity technologies against the adversary. I followed the participants' detailed experiences and reflections on cybersecurity technologies. Hence, for this study, I studied users' experiences in-depth and on their premises. The qualitative research interviews stand out in the field of Homeland Security with obvious methodological advantages. It is well suited to document not only user experiences from hands-on use of the technology but also reflections on non-use. Through interviews, I gained knowledge on everyday work and practices that are not striking or noticeable during observation of user situations.

Role of the Researcher

For this study, I was the interviewer and observer. The researcher is the primary research tool in a qualitative study. An interpretive study relies on the intensive experience of respondents as an observer-participant (see Creswell, 2009; Miles & Huberman, 1994; Patton, 2002). Hence, to prevent bias, it is essential to have a solid understanding of the material without a preconceived solution to the cybersecurity problem. I maintained an open mind to opposing theories and contrary evidence as recommended by Yin (2014). Also, I was able to minimize partiality by suspending personal value judgment in the process of gathering information. The study was designed with open-ended questions as a way for participants to present contrary opinions. I

identified a comfortable interview environment in a neutral location, and was open to contradictory evidence, with due regard to the cultural specificities of Nigeria that make this investigation unique (Moustakas, 1994; Yin, 2009). I had no personal or professional relationships with the study interview participants outside casual acquaintance via professional meetings and programs. I engaged personal contacts that were able to provide the necessary introductions to most of the participants. I addressed ethical values before the commencement of the interviews to advise participants about the voluntary nature of the project and their right to terminate interviews at any time.

No other ethical challenges were encountered. The interviews were voluntary and could have been terminated at the request of the interviewee

Methodology

I collected data for this study holistically. The data collection includes face-to-face interviews with security experts, document content analysis of open source/nonclassified materials; government threat assessment; Legislative Report on Terrorism; policy papers, peer-reviewed academic works, and journals. The study was qualitative research interviews, which was designed to find answers to how experts see the effectiveness of cybersecurity technology to mitigate terrorist propaganda and networking in Nigeria cyberspace. Rubin and Rubin (2012) confirmed that qualitative interviews remains one of the most common and vital data gathering tools in qualitative research. Qualitative research supports the “purposive” selection of key informants in the field who can assist in identifying information-rich cases (Creswell, 2009). With Qualitative research interviews, I focused on key players on how Nigerian government

manages the terrorists networking and propaganda in cyberspace. In the study, I examined experts' selection strategy and perceptions about the effectiveness and practicality of cybersecurity technologies. There were collections of multiple forms of data in a natural setting through semistructured in-depth face-to-face interviews. Also, I established a protocol for recording this information. Rubin and Rubin (2012) posited that the qualitative interview is appropriate when the study purports to answer "how" and "why" questions. Hence, I collected the needed data through a qualitative interview through which I assessed the effectiveness of cybersecurity technology from the professional experiences and perspectives of experts: which included law enforcement agents, intelligence personnel, cybersecurity experts, government officials, and private security administrators. Moreover, a qualitative method allows the researcher to view issues through a variety of lenses, which allow for multiple phases of any phenomena to be exposed and understood.

Population

The research population included Nigeria Law enforcement agencies, Intelligence Community, Ministry of Defense, Technology, the Office of National Security Adviser (ONSA), academia and the leading private sector telecommunications and internet infrastructure companies in Nigeria.

Sampling Strategy and Participants Selection Logic

Robinson (2013) recommended a four-point approach for qualitative sampling. The concept of the Point 1 is to define the sample universe, which for this study was all cybersecurity professionals and security administrators in Nigeria. This sample universe

included the Law enforcement agencies, Intelligence Community, Ministry of Defense, Technology, the Office of National Security, and the leading private sector internet infrastructure and telecommunication companies. The measures for the choice of research participants was based on the fact that the research participants would provide enormous and relevant information to the inquirer. I considered the willingness of the participants to partake in the process without any pecuniary benefits, including the availability and the accessibility to participants. In this study, I reached out to participants by the assumption that they had information and experience as law enforcement, communication technology, cybersecurity, intelligence, academic or counterterrorism experts to share.

The participants were selected in a manner that balanced the ideal with the practical. Given the scope, time and resources available, the study had to interview people from the spectrum of institutions involved. The third point was to identify the sampling strategy which was a purposive sampling of both public and private sector participants as discussed in Patton (2002). Purposive sampling enhances prompt discovery of relevant and comprehensible information and is useful for evaluating variations in how a phenomenon is viewed (Robinson, 2014; Suri, 2011). Also, I deployed a snowball sampling strategy, which entails the researcher to discover potential participants through interviewees to complement the purposeful sampling strategy. Both the purposeful strategy and the snowball sampling strategy did not require a definite number of participants to reach a saturation level.

The fourth point identified by Robinson (2013) is to source the desired sample, which entails the recruitment of the participants from the target population. Using the

inclusion and exclusion selection criteria and the time-resource constraints, the individuals who were selected for the interviews had a strong background and specialized knowledge in information technology, intelligence and operational implementation responsibility for cybersecurity issues. This method provided an opportunity for public and private sectors to be represented in the overall study sample, which is a fundamental requirement for using a purposeful sampling strategy (Robinson, 2013). In this study, I interviewed 15 professionals in the fields of cybersecurity, strategic planning, risk assessment, and law enforcement. I selected participants from law enforcement, cybersecurity professionals from both private and public sectors, and academic community. As earlier stated, the steps enabled the qualitative design to meet rigor, trustworthiness, thick, and produce rich data (Patton, 2004). The purposeful strategy also met the test of theoretical relevance (Thomas, Vilmos, & Peer, 2013).

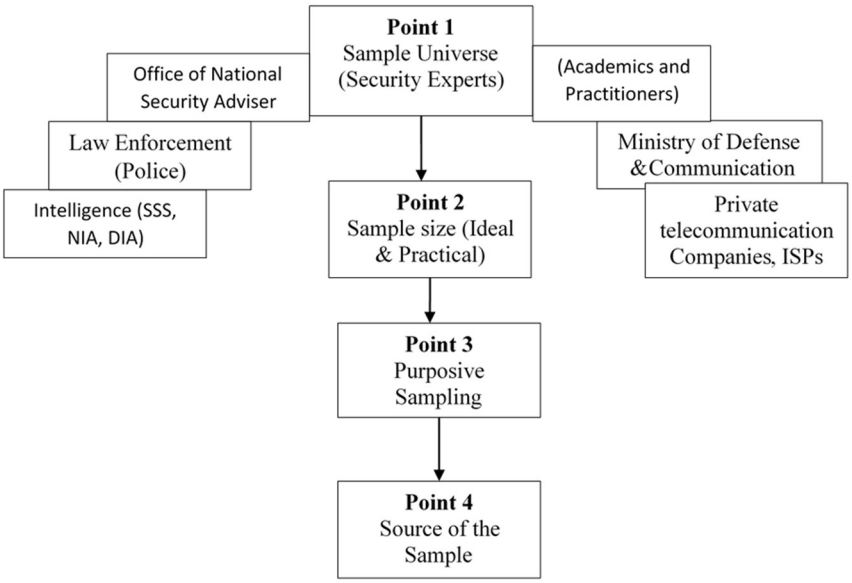

Figure 2. Four-point approach for qualitative sampling.

Analytical Strategies

The study conducted content analysis of open source documents, government threat assessments, legislation, policy papers and peer-reviewed academic literature and semi-structured interviews. The content analysis provided overview of policy, including the identification of the critical component of cybersecurity approaches to terrorism in cyberspace. Additional documents were collected during the fieldwork on current and planned government National Cybersecurity Policy. I offered a precise reading of a specific document set and sought to protect the authenticity to maintain credibility in the qualitative tradition. Furthermore, document review provides background information and historical insight to help the researcher understand the historical roots of particular issues (Glenn, 2009, p.30). In addition, it enables the researcher to contextualize data collected during interviews. Moreover, it can suggest some crucial questions that need to be asked and situations to observe as part of the research. Document review will enable researchers to track the trends and change in development which can help verify the findings. My goal was to give a truthful account of the information located in every document and to interpret the meaning found in them scientifically.

Also, inquiries must provide insight, which extends beyond the specific issues under study. Qualitative interviews rely on the researchers to assess the more extensive applicability lesson learn from the findings to achieve external validity. Hence, the results from the document analysis and qualitative interviews can be confirmed in that inferences can be traced back to the primary sources to corroborate the findings (Wesley, 2010).

Also, the results of the literature review were used to develop the interview protocol used with the participants. The interview protocol guided the findings from the first research question and second research questions on what the current thought regarding the role of technologies in fighting expansion and organization of terrorism in cyberspace, including what steps the Nigeria government is currently taking. The interview protocol is included as Appendix (B). The literature review also identified the current threat landscape and was used to make recommendations, including identification of gaps that exist between international best practices and the current policies and practices in Nigeria

The interviews were in accordance with the protocol approved by the Walden IRB. The interviews used open-ended questions and face to face interviews were recorded using a digital recorder for more accurate transcription. The researcher's comprehensive notes were used to supplement the transcripts. Interviews were conducted in the individuals' offices or at mutually agreeable places such as conference rooms, home office or Hotels. The duration of each interview was 45 minutes and sometimes lasted up to an hour. The transcripts were analyzed to develop an understanding of the current approach. All individuals who participated in the interview will receive a final copy of the findings of the study for informational purposes. The researcher intends to present the conclusions of the study in Nigeria at a yet to be determined date.

Data Collection

Data collection was accomplished by triangulation of evidence from document content analysis and the in-depth interviews. The purpose of using a variety of methods

was to capture the different dimension of the same phenomenon. Triangulation of information among various sources of data helps to achieve validity (Simon, 2011). The data included both primary and secondary sources.

The study's primary data collection was through a series of interviews. Also, Secondary data were collected by both manual and online method. The use of primary and secondary sources saved time and helped with the discovery of solutions to research problems (Creswell, 2009). All participants answered ten open-ended questions listed below about the topic of the study.

Table 2

Purpose of the Questions

Questions	Objectives
1. Let me begin with what you can tell me about the risks associated with terrorist organizations' messages of violence, and radical ideology in the cyberspace?	To probe the respondent's knowledge and understanding of the risks associated with terrorist messages in the cyberspace and what tools are used to propagate such messages.
2. What do you see as the role of technology in fighting expansion and organization of terrorism?	Probe the needs, IT capabilities, and the goal (people, process, and technology).
3. How would you describe the current level of understanding of this kind of cyber threat by senior government and private sector officials in Nigeria?	Explore the participants' experiences with cybersecurity technologies.
4. How would you characterize the ongoing efforts being undertaken to protect the Nigerian cyberspace from being entirely hijacked by the terrorist to spread a message of violence?	Discuss the role of government and the kind of technologies that have been identified by security experts to defuse the effects of terrorist expansionist agenda in the cyberspace.
5. What kind of technologies have been most useful to lessen terrorist networking in the cyberspace?	
6. How do you select such technologies, what is your testimony about its effectiveness, and how practical are the techniques without violating civil liberties, privacy and fundamental human right to free speech?	Focus on the practicality of the technologies used and the concern about their impact on individual rights and privacy (people, technology, and process).
7. What impact does such technologies have on privacy and individual liberties?	
8. What is (are) the authority (ies) responsible for cybersecurity strategy? Where is this determined/published?	Tackle the issue of leadership and authority responsible for providing guidance, including the additional measures in term of policies.
9. What additional measures and policies could the Government implement to incorporate international best practices into how to use technology against the adversaries?	
10. Is there anything else you will like to tell me?	A general comment and other valuable remarks that they would like to add within or outside the structure questions.

Data Analysis

This study used the theoretical framework of RAT developed by Cohen and Felson (1979). The choice of RAT was to understand the data from the perspective of the environmental place-based account that three factors must be present for any crime to occur. Therefore, I analyzed both primary and secondary data with the explanation of the three components (Motive, Opportunity, and Means) and associated by a causal link. Yin (2003) posited that researcher developed explanations regarding the research problem before linking them based on this method of data analysis.

Data were organized by research questions. This organization was done by sorting the data collected from document analysis and the in-depth interviews into an articulated format to infer causal links and connection of findings.

The raw data on the country was consolidated and synthesized into a coherent report. The analysis was densely dependent on the coding process used to pull together the essential items and findings from the various data forms. The NVivo qualitative analysis software was used to support coding and data analysis. The software allowed for better identification of themes and patterns in the document review and the fieldwork, and it built on the work done with NVivo during the literature review. The study used an on-going, iterative data analysis strategy as recommended by Ravitch and Carl (2016) The approach allowed for adjustment of the interviews as new threads developed and patterns were detected. Pre-coding based on the literature review was used, and I was

able to employ pattern coding as the process proceeded. The software tools proved helpful at this stage.

Issue of Trustworthiness

In all kinds of research, it is necessary to authenticate the reliability of the information generated by the investigation. Credibility, transferability, dependability, and confirmability are the essential issue of trustworthiness in any study. Therefore, it will be impossible to reconstruct the research and repeat the result without a valid, auditable trail. This study incorporated multiple sources, including document content analysis, in-depth interviews, and observation to make it credible. Yin (2009) recommended three tactics as a way of addressing construct validity: (1) use multiple sources of data, (2) establish a chain of evidence, (3) and use key informants as casual reviewers as the product emerges. For this study, I used documents, which are peer-reviewed journals and vetted government sources. I conducted interviews with key players in both the public and private sectors. I consulted key interview participants as the study emerged to assess the validity of the findings regarding the perception of individual security experts on the effectiveness of cybersecurity technologies in mitigating terrorist propaganda in the Nigeria cyberspace. I used doctoral level coworkers to conduct in progress peer reviews to ensure both academic rigors of the investigation and credibility of conclusions. The research is externally valid and transferable per the sampling model.

Internal validity was very crucial as it is essential in an exploratory qualitative study where a global south nation like Nigeria was assessed for application of various strategic approaches and recommendations to enhance its cybersecurity. Yin (2009)

advised researchers to use the data analysis phase of the research to look for patterns, build explanations from the emerging trends, and address rival or non-concurring interpretations. In this study, I used RAT lens to assess what Nigeria is currently doing to respond to the challenges in terrorist organization propaganda and networking in light of the three dominate cybersecurity paradigms. I made recommendations on where the country might take further actions in term of response and preparedness. During the data analysis phase, the material generated from the literature and document review were used to establish the key coding parameters. From these coding parameters and subordinate codes, I categorized and coded the data to match with the different patterns and continually assessed the material to detect patterns and rival explanations.

Moreover, Yardley (2000) and Robinson (2013) pointed out that the precise identification of the sampling strategy is useful in defining the rigor and transferability of the study. Luiijf et al. (2013) revealed that the individual elements of national cybersecurity strategy vary and are inclined to the cultural and worldview of the nation promulgating a specific policy. Hence, the outcome of the similar study in another country will likely vary, but the process can be transferable. Interviews with similarly placed individuals would be useful in describing how that second nation is positioned for cybersecurity strategy against cyberterrorists. This specificity in describing the sampling strategy enhances transparency and confirmability (Robinson, 2013). Those results could then be applied to the same set of approach, which has been developed by assessing a more significant number of nations and institutions.

This study was a qualitative research interview. Therefore, the alternative means of assessing external validity, replication, was not practical but may form the basis for additional research in a follow-on study.

Ethical Considerations and Human Subject Protection

In this study, I followed the guidelines of the Institutional Review Board (IRB) of Walden University to avoid ethical pitfalls. Prior to conducting the research, a review of the methodology was conducted by IRB for authorization and approval. Also, I completed National Institute of Health (NIH) Office of Extramural Research's "Protecting Human Research Participants" training.

The participants in this study were adults who work with public and private organizations. Their participation was voluntary, and anyone who felt uncomfortable was allowed to opt out of the exercise. Research ethics guide social science researchers on research that involves human participants (Kim, 2011). Hence, in this study, I adhered to all necessary ethical standards to maintain integrity, credibility, and validity (Creswell, 2009). The effect of the investigation and the study, including the principles and consequences of sampling, process, and interpretation are closely related to confirming the validity. There was no known harm connected with partaking in this study beyond normal workday stress. Every member participant was assured of confidentiality and completed a mandatory consent form before the commencement of the interview. Therefore, the participants were protected by keeping their identities in a nonattribution format. Also, files, audiotapes, and transcripts were stored in an encrypted digital format on an external drive and cloud-based server. External storage serves as a backup in case

of failure from primary computer. Furthermore, personal identification information was redacted from the transcripts before data validation. Selected participants who assisted in validating the results and research were the only group who had access to the transcripts. Copies of the Consent to Audiotape and Statement of Confidentiality can be found in Appendix C.

Research data will be kept for five years from the completion and acceptance of the final dissertation and then destroyed. Digital copies will be maintained for five years before deletion. The Hard drives containing personally identifiable data will be cleaned and destroyed at the end of the life cycle.

The study was not done in my current work environment or with any close personal associates. I conducted all interviews professionally as I have done for previous work-related research efforts involving personal interviews and observations.

Summary

Terrorism was the central phenomenon I addressed in this qualitative interview study, with a focus on cyberterrorism and the role of cybersecurity technologies in fighting the expansion and organization of terrorism in Nigeria cyberspace. The research population comprised members of law enforcement agencies, the intelligence community, academia, military, legislators and cybersecurity professionals in public and private sectors.

For this study, my role was as an interviewer and observer. Data collection was accomplished by triangulation of document, which included document content analysis and face-to-face in-depth interviews. The research interviews were used to explore the

views, experiences, beliefs, and motivations of experts, to evaluate the effectiveness and applicability of cybersecurity technologies against terrorists' propaganda activities in the cyberspace. Also, data analysis was through coding and use of NVivo software application. No ethical issues were faced in this research. I followed IRB procedures required by Walden University while conducting this research (see Appendix A, B &C). The findings of my study are in Chapter 4.

Chapter 4: Results

Introduction

In this qualitative research, I revealed the facts and circumstances related to the role of technologies in fighting the organization and expansion of terrorism in cyberspace from security experts' perspectives. In this study, I presented the testimony of 15 security experts, using qualitative interviews to appraise the role of technologies in fighting the expansion of terrorism in Nigeria cyberspace. The participants were familiar with the Nigerian cybersecurity and counterterrorism campaign planning and strategy, including capabilities and Nigerian perspectives. They were selected to provide descriptive information concerning the effectiveness and practicality of cybersecurity technologies in combating terrorism in cyberspace. The study was aimed to answer two primary research questions, which guided the interviews:

1. How do the experts see the role of technology in fighting expansion and organization of terrorism in cyberspace?
2. How do experts perceive the effectiveness and practicality of cybersecurity technologies as a tool to mitigate terrorist propaganda and networking in cyberspace?

I used in-depth interviews with open ended questions to provide answers to the research questions. Also, the study includes a qualitative content analysis of open source/unclassified documents, including infrastructure information, legislation, policy documents, terrorism report, peer-reviewed academic works, and journals. Progressive axial and selective coding schemes were designed and validated the data through

methodological triangulation. The approach enabled me to conceptualize themes and analyze the data through a Routine Activities theoretical lens. The findings are organized by themes relevant to the research questions and the theoretical propositions.

Nigeria is adjusting its national cybersecurity strategy to confront cyberthreats resulting from terrorist expansion and coordination in cyberspace. In this study, using interviews with key individuals in academia, and the public and private sectors, I was able to collect information as a basis of making recommendations to the government of Nigeria.

The first question about the role of technologies in fighting the expansion and organization of terrorism in cyberspace helped to establish the baseline for policy development and coalition against terrorism in cyberspace. The second question was essential to examining and assessing the status quo for making comparison of the response to terrorists' expansionist agendas in cyberspace using cybersecurity technologies. The result of Research Question 2 formed the basis for the recommendations outlined in Chapter 5.

As a qualitative interviews study, the setting and demographics of the interview sample were outlined, including the data collection and analysis procedures used in this chapter. Lastly, the results are presented in line with the two research questions.

Setting

After the approval of the research proposal by the Walden IRB in May 2018, a research trip was planned to Abuja for early May 2018. The approval number for the study is 05-01-18-0543869. The process of contacting interview participants started in

early May 2018 in collaboration with my contacts in Nigeria. The plan was to identify other potential interview participants from outside the primary network. I spent a total of four weeks in Nigeria with most of the interviews conducted in Abuja and the rest held in Kano, Lagos, and Warri based on the preferred location of the participants. Obtaining interviews with personal contacts in government and academia was easy, whereas it was challenging getting to speak with people in the private sectors. One critical observation is that Nigerian security agencies depend more on foreign technology companies in addition to telecommunications organizations, which are vital to national security. The interviews were conducted face-to-face, and on two occasions I asked some follow-up questions via telephone.

Upon arrival in Abuja, final interview arrangements were made with some key government officials, representing the ministries of interior, communication, defense, and information. In addition, one of the interviewees assisted in identifying a knowledgeable participant at the Office of the National Security Adviser (ONSA). I was able to interview two members of the Nigerian National Assembly. My contact in Abuja was able to secure an appointment for me to meet with participants from the Nigerian Police, the Department of State Security Services (DSS), and the Nigerian Army. The participants expressed willingness to assist in this study and majority of them showed a level of enthusiasm, supporting the fact that the investigation is timely, relevant, and vital based on the current trend of terrorists' operations in Nigeria. Therefore, it was an opportunity to obtain enough information and clarification to support the research. Some of the face-to-face interviews were conducted in individuals' offices, hotels, and homes.

Four participants were interviewed in a conference room provided by one of the ministries and located in the building where they work. The participants selected the interview sites and we ensured there were no disturbances during the discussions. The office interview enabled me to observe the level of sophistication of cybersecurity technology practices that are being deployed in different agencies. The observation enabled me compare the level of preparedness, understanding, and application of cybersecurity technology in Nigeria in comparison to the countries of the global north, especially the United States.

Demographics

The participants of this study consisted of fifteen professionals working at the middle- to upper-management levels in the fields of cybersecurity, counterterrorism, law enforcement, military, and intelligence organizations. They also comprised public officials, members of the academic community, and private telecommunications companies. The Nigerian Police, where the sample was drawn, is the principal law enforcement agency in Nigeria with approximately 350,000 police officers. The participants were both male and female ranging in age range from 40s to 50s and had different educational backgrounds and experiences. The government officials were not primarily security experts but rather the individuals tasked with passing legislation and developing and implementing policies to advance the security of the nation and its interests. They have education inclined toward law, policy, and national security affairs, which made them contributed meaningfully to the topic. Also, the law enforcement, military, intelligence, and private sector participants had much stronger technical

backgrounds and had experienced advanced training in cybersecurity. The participants from academic communities offered more insights into ethics and civil liberties. It was important to include this diversity of backgrounds to acquire contrasting points of view in the study in order to assess the practicality of the measures being taken and their potential effectiveness in achieving the goal of fighting the expansion and organization of terrorism in cyberspace. The variety of participants allowed triangulation of the results from different sectors. This information is important to provide context for the gap analysis of RQ 2 and the recommendations for action in Chapter 5.

The personal information of all participants was kept confidential using alphanumeric code (pseudonyms AS1 to AS15) to protect all their identities. Table 3 shows the participants' demographic information, which enabled me to develop answers for RQ1 and RQ2.

Table 3

Age and Profession of the Participants (*N* = 15)

Participants	Age	Profession
AS1	40s	Cybersecurity (private sector)
AS2	40s	Strategic planner/legislator
AS3	40s	Risk assessor
AS4	50s	Lawyer/law enforcement
AS5	40s	Emergency planner
AS6	50s	Information security specialist
AS7	40s	IT security director
AS8	50s	Lawyer, legislator
AS9	40	Army/security specialist
AS10	40s	Counterterrorism expert
AS11	50s	Communications expert
AS12	50s	Academic
AS13	40s	Intelligence, historian
AS14	40s	Intelligence director
AS15	50s	Professor, computer scientist

Data Collection

The 15 participants were recruited to participate in the study in May 2018 as proposed after the IRB gave approval to proceed with the research. All 15 personal interviews were completed during a four-week period in May 2018. Ten of them were conducted in Abuja, one in Kano, three in Lagos, and the last one in Warri, Delta State, Nigeria. The questions in the oral interviews were identical, while follow-up questions varied based on earlier responses of each participant. The completed interviews with all participants were denoted with alphanumeric code names AS1 to AS15. The face-to-face interviews were recorded using a Samsung S9 phone running Voice Record Pro software with simultaneous longhand notes. I took the advantage of the opportunity to watch and observe varieties of technologies and the state of cybersecurity readiness. The duration of each interview was 45 minutes. Follow-up calls were made to three participants for clarification, which led to some modifications in their responses.

The data collection proceeded as proposed. The public sector participants, which included law enforcement agencies, intelligence organizations, the military, and policy makers represented a cross-section of individuals involved in developing and implementing strategies to counter terrorist threats in Nigerian cyberspace. Therefore, the interviews included both career officials and political level policymakers. The participants met the objective of a purposeful sampling discussed in Patton (2002) and Creswell (2007). The government personnel were employees in multiple ministries and were responsible for the development and implementation of security strategy. Participants from the private sector were also in charge of developing and implementing

corporate policy in line with government strategy and regulation. The academic sector participants with backgrounds in counterterrorism and cybersecurity added insights that were useful in triangulating the data.

Data were also collected from the content of written documents, including:

1. Nigeria National Security Strategy on Cybersecurity.
2. Legislative Report on Terrorism.
3. Conference Materials from Nigeria National Security Summit.
4. Nigeria Police Crime Alert.
6. Speeches and Remarks by Senior Government leaders on National Security.
7. United States Department of State Country Reports on Terrorism (2016).

Data Analysis

The data analysis was carried out in an iterative and repetitive process as recommended by Ravitch and Carl (2016). The iterative process existed in the data analysis used in this qualitative interview study as each interview was reviewed at least three times. This repeated review of the interviews enabled me to identify recurring themes and concepts, which then informed the coding process. The interview data were analyzed using the following steps:

(1) Familiarization with the data by listening to the recorded data thrice to develop a general initial impression. (2) Transcription of the interviews. (3) Reading of the interview transcription twice to form a full picture. (4) The initial list of codes was developed as they emerged from the interviews. (5) Analysis of the raw data by assigning codes through NVivo, which identified nodes that represented the reoccurring patterns.

Consequently, the nodes were clustered into three themes: (1) technologies, (2) terror in cyberspace, and (3) cybersecurity. Under the three new subheadings, the nodes were more manageable and easier to organize. Using NVivo), the ten interview questions were linked to 33 original codes and ultimately sorted into three code families aligned with the two research questions. This structure proved to be useful for visualizing the key findings.

While conducting the interviews and analysis of the materials, it became apparent that cybersecurity is an issue of interest and concern in Nigeria, although with varied motivations .

Among the 15 participants, one gave answers that seemed somewhat outside the norm in comparison with the other 14 participants. When his answers were consistent with the others, I considered them. Also, when they were different, those responses were considered to be outliers and treated as discrepant.

Evidence of Data Trustworthiness

The data for the study achieved credibility, transferability, dependability, and confirmability strategies as proposed with no adjustments. Credibility was accomplished by incorporating multiple sources, including document analysis, observations, and face-to-face in-depth interviews with a diverse participant sample. The reputations of the participants are impeccable and their submissions were reliable based on the nature of their jobs and years of experience. The stringent adherence to the interview protocol supported the strength of a semi-structured qualitative interview methodology. It promoted data consistency, including the depth of exploration with probing follow-up

questions. Dependability, reliability, and validity were achieved by triangulation. Also, confirmability was accomplished through reflexibility. As data were analyzed, explanations were built and associated by a causal link. During the data collection phase, the initial findings and emerging themes were discussed with a Nigerian counterterrorism expert who confirmed that Nigeria follows the United States' model in combating terrorist activities in cyberspace. Moreover, the initial findings were circulated to the participants and third-party experts for assessment and comments before completion of the study. The comments received were supportive of the findings. With all these steps, other researchers would be able to follow the same study methodology and advance their ability to confirm the results.

Internal validity was achieved through continuous assessment of the data, which helped to identify patterns and themes. The repetition of themes by multiple participants strengthened the findings. Although participants viewed most of the questions in the same way an individual's position and professional background tends to influence how they perceive issues, they all recognized terrorists' expansionist agenda in cyberspace as a problem. The study achieved external validity based on the analytical model, which promotes transferability to the global cyberterrorism problem. The data analysis along the global threat landscape and general doctrine on cybersecurity make the model applicable to other cyber response planning contingencies. Also, the literature review was developed within a global context and the model provides a framework that expedites a comprehensive peer review.

All interviews used the same questions to ensure dependability. The questionnaire influenced the coding process and aided in the organization of the data. The interviews provided more information and the ability to identify non-verbal clues. The use of digital recording and transcript review enhanced the dependability and confirmability of the data generated from the interviews.

Results

The data obtained from the participating experts was analyzed and interpreted to understand the role of technologies and their effectiveness in mitigating the expansion and organization of terrorism in cyberspace. Each theme is presented alongside relevant participants' comments and these results led to the recommendations found in Chapter 5.

The participants of the qualitative interviews were security professionals from either the public or private sector. They were responsible for cybersecurity issues in Nigeria. The results section begins with the participants' interpretation of policy and guidance related to the use of technologies and their applicability. Also, the description of those guidelines reflected the integration of cybersecurity methods in the counterterrorism approaches pursued by each participant based on their agency affiliation. The primary research tool was a ten-question interview designed to provide information to answer the two research questions: (1) How do experts see the role of technologies in fighting expansion and organization of terrorism in cyberspace? (2) How do experts perceive the effectiveness and practicality of cybersecurity technologies as a tool to mitigate terrorist propaganda and networking in cyberspace?

The participants' assessments of the real-world contextual environment gave insights into planning priorities, including capability development, governance, risk and mitigation, and civil liberty concerns. The appraisal enabled the study to identify the essential solution and method to apply.

Capabilities and Role of Technologies (Q.1)

Research Question 1 focused on the views of experts on the role of technologies in fighting terrorist networking and expansion in cyberspace. I used the following questions to probe for details;

1. Let me begin with what you can tell me about the risk associated with terrorist organizations' messages of violence and radical ideology in cyberspace?
2. What do you see as the role of technology in fighting the expansion and organization of terrorism?
3. How would you describe the current level of understanding of this kind of cyberthreat by senior government and private sector officials in Nigeria?
4. How would you characterize the ongoing efforts being undertaken to protect the Nigerian cyberspace from being entirely hijacked by terrorists to spread a message of violence?
5. Which authority/ies is/are responsible for cybersecurity strategy? Where is this determined/published?

6. What additional measures and policies could the government implement to incorporate international best practices into how to use technology against terrorist adversaries?

The interview questions listed above were asked in every interview while the follow-up questions varied for individual participants because interviews progressed differently. I asked follow-up questions, including probes about the limitations of technology; availability of experts to manage and deploy those technologies; civil liberties and privacy concerns; end-user licenses of sophisticated technologies; risk assessments of cyberterrorism; threat identification; communication of risks; awareness of cyberthreats, and consequences of intrusive technology on fundamental human rights.

While information and communication technologies have created a new avenue of terrorism, they also provide modes for defense. Cybersecurity technology is most useful in preventing terrorist messages and intercepting their communications before they reach a site's visitors; and, government should use technology to disrupt terrorist networking in cyberspace, one of the top three threats to national security.

The views of Security Experts

All the interview participants considered technology a vital tool in counter-extremists' cyber activities. They indicated it would require technology such as surveillance, specialized cyberweapons and tactics to confront the threat of terrorism in the cyber domain. Social media, including Facebook, Twitter, WhatsApp, and YouTube, are commonly used to network among potential terrorists in Nigeria. According to the

interview participants, the most needed for counter-cyber activities terrorism were (cyber) surveillance technologies.

As noted by Rosand (2003), the terrorist threat has evolved over the last few years into a new phase due to changes in technology. All the experts interviewed argued that the Nigerian government has become better at preventing sophisticated physical attacks, leading terrorists to the less complicated act of using cyberspace to propagate terrorism. The most noticeable shifts in the world of terrorism and counterterrorism in recent years have involved the more sophisticated use of the Internet and social media by terrorists to spread propaganda and mobilize support for their ideology. According to all the experts interviewed, the current action of the terrorist groups operating in Nigeria reflect the worst fear of law enforcement and counterterrorism officials. Their primary concern is the influence of terrorist messages, which can inspire people who are not known to exhibit any visible signs of radicalization or evidence of direct contact with terrorist organizations to obtain weapons and stage attacks against their communities. Sauter & Carafano (2012) posit that emerging technologies open windows for cyberterrorism while improved technologies play a significant role in fighting terrorism in cyberspace.

According to the experts interviewed, they observed that most of the law enforcement and intelligence agencies have standard practices and technologies in their routines. However, they have limited ability to process all the information from the centralized system to achieve security goals. The respondents unanimously pointed out that effective application of technology requires coordination between agencies. The coordination relies on intelligence management, a central authority, and leadership.

Participants interviewed argued that Nigeria as a nation faces myriad threats on a daily basis. It is thus essential to have a complete view of the terrorist operations and security threats in the cyber domains at all times. Law enforcement and intelligence agencies need to use various technologies to achieve success by detecting what may take a longer time for a human to identify. They need to program their systems to detect unusual activities and collect intelligence that is useful to thwart terrorist agendas and halt the expansion of terrorism in cyberspace. The participants pointed out that the current challenges open up new vistas of the opportunity of technology innovation and invention in Nigeria's security industries.

Significance of terrorist threat through cyber activities.

Documentary evidence reaffirms that the government of Nigeria considers terrorism as a significant threat to both the nation's economy and national security. The Nigerian government is making concerted efforts to combat terrorism in cyberspace through various programs, including the National Cybersecurity Policy Summit. One of the factors that foregrounds the issue of cybersecurity is the activities of the Boko Haram terrorist organization in Nigerian cyberspace. Boko Haram is a terrorist organization with Islamic religious inclination, which emerged in the Northeast of Nigeria in 2002. The official name of the group is "Jama'atul Alhul Sunnah Lidda awati wal Jihad", which means those who are committed to the propagation of the teachings of the prophet and jihad (Mechan & Speier, 2011).

AS1 pointed to how the group used technology to spread propaganda when it kidnapped schoolgirls in 2014. The activities of Boko Haram have affected Nigeria's reputation globally. The group has adopted the method of using new media technology, especially YouTube, to broadcast its activities to the public. Most of the participants corroborated the working definition of cyberterrorism for this study, which is terrorists' use of cyber technologies to recruit, train, plan, and fundraise with the purpose of instilling fear so that targets would comply with their demands or ideology. According to all the participants, terrorists use social media technology: "the first line of action against them should be cybersecurity technologies to disrupt, monitor and deter their activities in cyberspace". AS1, a cybersecurity expert, stated.

The following passage from the interviews with AS2, AS4, and AS9 best highlight the threat of cyberterrorism and the use of technology for counter action:

> Researcher: What are the risks associated with terrorist organizations' messages of violence and radical ideology in cyberspace?
>
> All the participants concurred that it is a reputational risk. The activities of Boko Haram have affected perceptions about Nigerians and the country's image. As AS1 explained, "the reason Nigeria looks at terrorist online activities and cyberterrorism is because our image is being affected". The reputational risk arising from terrorist broadcasts with new media technology and other associated cybercrimes is having negative effects on business and tourism as mentioned by AS6, AS9, AS10, and AS15.

The answers provided aligned with the declaration in the Nigerian cybersecurity document that the online activities of terrorist organizations in Nigeria "adversely affect the country's economy as well as individuals and organizations within Nigeria's physical territorial boundaries from financial, reputational, security and privacy perspectives" (Office of the National Security Adviser [ONSA], 2014).

AS2: Technology is useful to deal with cybercrime and the enemies in cyberspace. It is essential to use technology to fight terrorist organizations because their primary tools are new media technology. Boko Haram that denounces Western education uses technology, which is a product of western education as their main weapons against the public.

Role of technologies and how to use technology

The government and security experts are aware of the role of technology as significant tools in fighting the expansion of terrorism in cyberspace. Two of the participants from academia posited that cybersecurity technologies provide an excellent avenue for combating the expansion and organization of terrorism through cyber activities in Nigeria. The assessment of the experts pointed to the fact that government efforts had already been geared toward the use of cybersecurity technologies as the most viable weapons against terrorist activities in Nigerian cyberspace.

A recent assessment of terrorist capabilities in Nigerian cyberspace indicated that cyber jihadist and other armed groups are limited to using cyberspace for propaganda, raising money, and coordination (ONSA, 2014). Terrorist groups also use cyberspace to

commit crimes such as identity theft, web defacement, and denial of service (Osho & Onoja, 2015). However, Boko Haram has not demonstrated that the group has the knowledge and skills to conduct highly damaging attacks against critical infrastructures. Few of the respondents pointed to the fact that most of the terrorist groups in Nigeria are likely to rely either on single individuals with moderate technical skills or on foreign allies to assist their cyber campaigns. For instance, the Islamic State of Iraq and ash-Sham (ISIS)-West Africa relies on support from the parent organization, ISIS for cyber operation and propaganda. Hence, the government aims to leverage the terrorists' propaganda and networking online by gaining a technological advantage over them in cyberspace. With the resources currently available to the government, including international alliances with the Global North for technology and knowledge transfers, the government has the upper hand over terrorist groups in using technology for cybersecurity.

According to the respondents, several technological mitigation tools could be implemented, including content monitoring and cyber surveillance technology. The cyber mitigation strategies with the application of technologies are employed to achieve the goals of prevention, deterrence, detection, and response. For instance, cyber communication surveillance has a capability for intelligence collection with the ability to capture over twelve million data in a day. Tactical communication tools such as spyware, malicious software, and centralized monitors are used for intelligence collection, which could be processed to thwart terrorist agendas before they are implemented. Communication surveillance tools are sophisticated and can monitor networks, emails,

web addresses, phone calls, and text messages. Although Privacy International (2018) argues that any automated communication surveillance would amount to interference with the right of privacy, its significant advantage is that it is less intrusive as a human does not need to read the intercepted communication except it is required.

The Nigerian government has initiated a partnership with giant technology companies such as Facebook, Google, and WhatsApp to expand resources and technology to fight the expansion of terrorist content and propaganda in cyberspace. Privacy International (2018) describes four categories of communication surveillance, which include internet monitoring, mobile phone monitoring, fixed line interception, and intrusion technology.

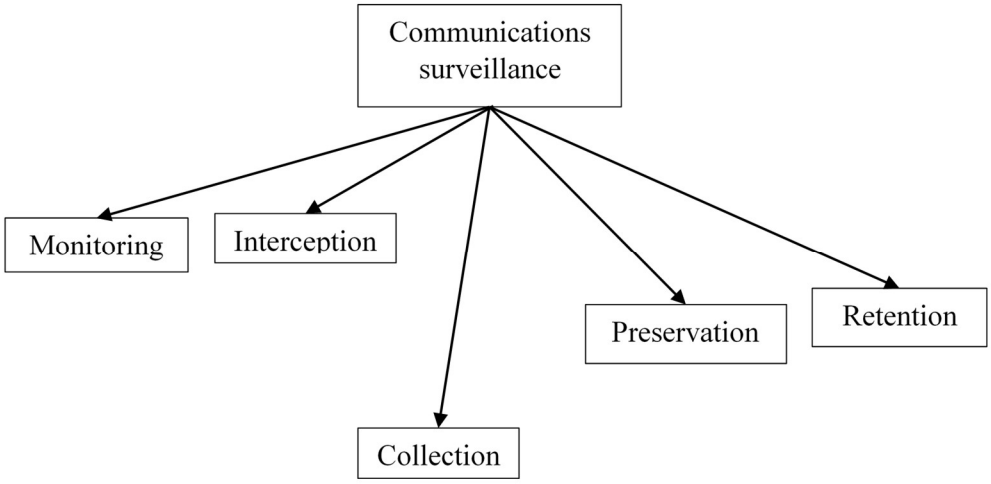

Figure 3. Potential functions of communications surveillance.

Barriers to fighting cyberterrorism activities through technology

AS15 explained that Nigeria needs to fund cybersecurity education to groom skilled personnel with expertise to defend its cyberspace from terrorists and non-state actors. The country is in dire need of "highly qualified software writers and hackers with skills that can counter terrorist websites". In the interim, the security agencies should fund programs that attract talents and encourage innovation. Law enforcement agencies should recruit skilled personnel who must be able to develop and produce systems capable of carrying out activities in cyber space. Also, it is essential for the Nigerian government to develop cooperation on a global scale in order to detect and prevent informational and technological threats to peace.

Limitation of Technologies.

AS8: Technology is not a total panacea. The approach must encompass "people, process, and technology". The first limitation of technologies is the risk of misconfiguration: human effort is required to configure cybersecurity tools to achieve desired security goals. This means that technologies get compromised when humans get compromised. Also, technology always provides an idea, but the onus is on intelligence agencies and law enforcement to join the dots to prevent potential attacks. Protection of cyberspace from adversaries is not guaranteed without the application of multiple approaches, including training and awareness. Vulnerable technologies, infrastructures, and methodologies could be exploited. 21st-century terrorists are technologically savvy

and tend to create alternative methods to implement their nefarious agenda. Hence, a complete strategy must encompass policy, procedure, and technology.

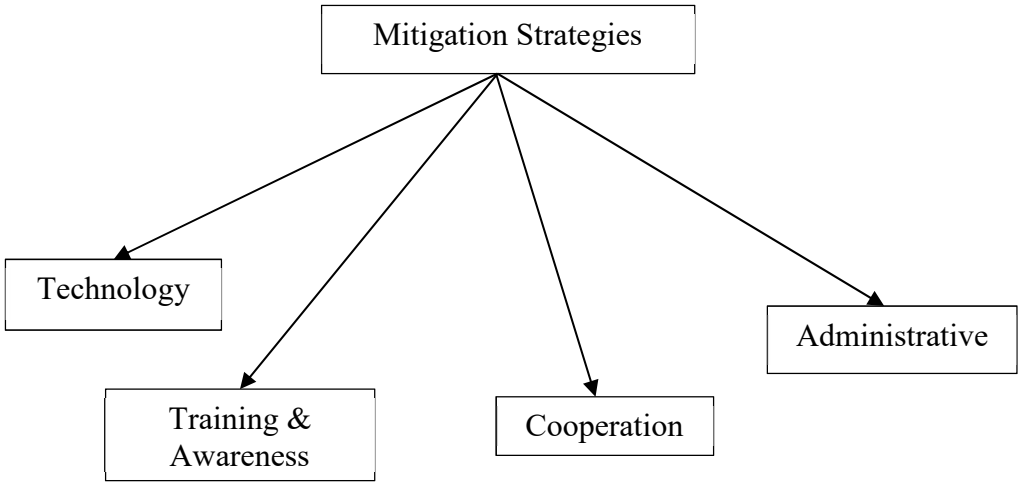

Figure 4. Mitigation strategies.

Current Understanding and Government Efforts

The interviews revealed that government understands the threat but is not committed enough to tackling the effects of terrorism in its cyberspace. From the government point of view, AS4 defined cyberterrorism as "an act of using technologies to communicate violence, train, plan, and target potential victims to influence government decision [sic] or to force an ideology on them." The definition conforms to the working definition for this study as identified in the literature review. Also, AS11 posited that "all of us are familiar with what "terrorism" means, but when we attach the word "cyber" with it, things get a bit more confusing." Nigeria's government accords higher priority to people who make political statements against government leaders on social media than

those who use new media technology to perpetrate violence. According to AS11, "they go after those who publish and expose corruptions in government on the social media." All participants explained that there is an ongoing effort on the side of the government, but the attention of the authority has been more valuable in tackling cybercrime. Institutions like the Economic and Financial Crimes Commission focus more on cyber activities related to financial crimes and crimes of opportunity, popularly known as "Yahoo Yahoo" or "419" in Nigeria. The understanding of the threat by policymakers galvanizes support and justification for the deployment of technologies to fight the expansion of terrorism in cyberspace. The role of technologies is essential for intelligence gathering to support security agencies' decision-making process to thwart terrorist agendas.

Government's role in fighting terrorist cyber activities. The participant experts working in both the public and private sectors believed that the government approach towards fighting terrorism in cyberspace must change from the traditional method of handling crime. At present, government agencies manage terrorist online content and propaganda in cyberspace like cybercrime where law enforcement investigates after a crime occurs. For instance, AS4, AS6, AS9, AS10, AS11, and AS15 informed that senior government officials understand the threat clearly. All interviewed participants hold that terrorism is both an economic and national security issue. According to AS14, "it [has] impacted business, scared away international investors and tourists; caused damage to [the] nation's reputation among the comity of nations; caused disaffection among communities and ethnic groups in Nigeria; and threatened Nigeria's existence and created

an atmosphere of insecurity." Five of the participants interviewed suggested a similar body like the Center for Strategic Counterterrorism Communication in the United States of America, which focuses primarily on countering extremist and terrorist propaganda in cyberspace.

Terrorist cyber activities in Nigeria. According to AS15, "before [the] February 2015 election, Boko Haram threatened some section community [sic] on [sic]YouTube broadcast not to go out to vote or face the consequences, and about 50 per cent of the community complied to the order for fear of terror repercussion." Also, the participants cited instances of when the secessionist group known as the Indigenous People of Biafra operating in the eastern part of Nigeria used social media to propagate the lie that all agricultural products, especially beans coming from the northern part of Nigeria had been poisoned. The propaganda affected commercial activities in the country as people opted to stop buying all food items coming from the northern part of Nigeria in the markets. As noted by Tugwell (2017), propaganda and terrorism go hand in hand as they both seek to control and influence their target in ways that benefit the sponsor. The purpose is to induce fear and uncertainty. Terrorist messages in cyberspace have fueled ethnic crisis leading to communal conflicts, arson, killings, maiming, and the destruction of cities in Nigeria. This action is a "threat to Nigeria [sic] national security; the information of operation of adversaries in our cyberspace is capable of breaking Nigeria", stated AS10.

All the participants agreed that terrorists use propaganda to misinform and disorient the public. The terrorist and separatist armed groups operating in Nigeria use social media and cyberspace to spread misinformation, propagation of violent ideology,

and for recruitment. AS14 who is a key leader in the intelligence community claimed the long year of tracking terrorist groups' activities shows that fundraising activity is the lowest priority observed among terrorist threat actors in Nigerian cyberspace. AS4, AS6, AS9, AS10, AS11, AS13, AS14, and AS15 corroborated the opinion that terrorist groups in Nigeria, especially Boko Haram, have another secret method of raising money outside social media. They know it will be easy for the authorities to trace their funds if they use social media. Their priority on the social media is thus to spread lies capable of influencing peoples' opinion or manipulating them into taking actions against the government. Therefore, the relevant authorities should develop cyber strategies and capabilities to confront enemies in cyberspace.

Table 4

Names Provided by Interviewees of Selected Terrorist Organizations and Separatist Movements Known to Be Active in Nigerian Cyberspace

Organizations	Categories	Modus (Website/Social media
Boko Haram	Terrorist organization	Uses YouTube, Twitter, and Facebook and has an official web page in the form of a blog12 through which it publishes its propaganda and recruits members. http://www. usufislamicbrothers. blogspot.com
Indigenous People of Biafra (IPOB)	Nigeria government designated IPOB a terrorist organization on September 20, 2017	Active on the social media for recruitment, fundraising and incitement. The group has official website: www.ipob.org
Islamic State West Africa and the Movement for Unity & Jihad in West Africa	Terrorist groups; both offshoots of ISIS and Al-Qaeda in the Islamic Maghreb	Social media platform. www.youtube.com
Movement for Actualization of the Sovereign State of Biafra	Separatist movement	Active on social media: https://www.facebook.com/Massob-170125269761711/. Website: http://massob.biafranet.com/
Movement for the Emancipation of the Niger Delta	Separatist movement	Social media platform. www.youtube.com

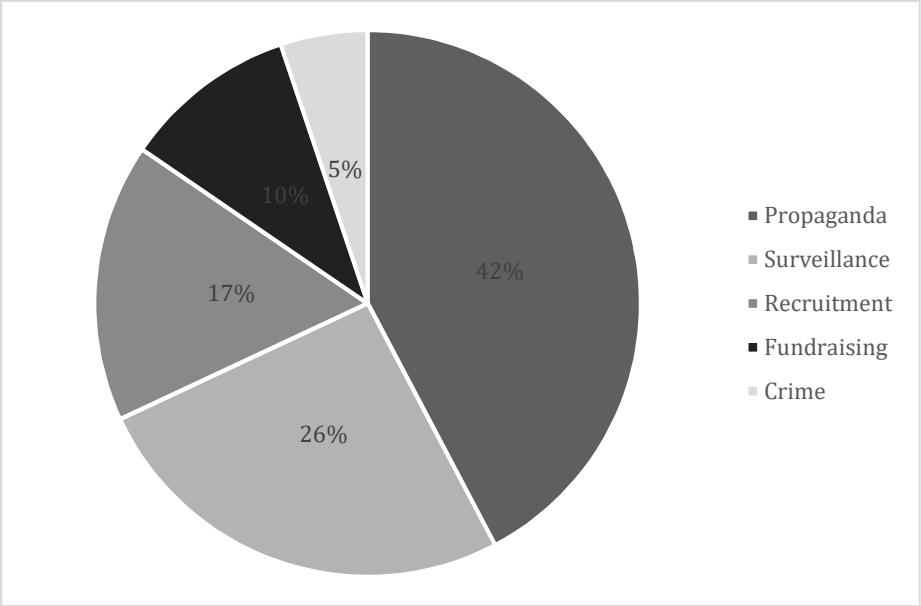

Figure 5. Cyber activities of Nigerian terrorists identified by interviewees.

National Cybersecurity Strategy

The sections of this policy document related to the prevention of terrorist messages and propaganda in Nigerian cyberspace explain the position of the Nigerian government on the adoption of "a risk management-based and technology neutral approach in performing assurance activities." Therefore, it is considered as the official guideline which security experts follow in all situations.

The document defines cyberterrorism as "activities that involve the use of computing and cyber technologies in aiding or executing terroristic activities of any form" (ONSA, 2014).

The document reveals the level of readiness to keep cyberspace safe from cyberterrorists. As pointed out, the "National Cybersecurity Strategy is the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical

information infrastructure, and building and nurturing a trusted cyber-community" (ONSA, 2014). As noted in the document, the jihadist cyber threat tops the list of threats that confront Nigeria. Also listed are criminal activities such as cybercrime, fraud, child online abuse and exploitation, cyber-espionage, and cyber conflict.

Key approaches to a successful national cybersecurity program are identified to be public and private sector partnership, multi-stakeholders engagement, and international cooperation (ONSA, 2014). Similarly, AS3 and AS4 were united in their opinion that Nigeria's leaders "are concerned over anything related to terrorism and the cyberspace. The security agencies in the country have been ordered to be prepared and to build resilient systems by closing the gap between law enforcement, intelligence, and national security." AS12 disagreed at the level of leadership commitment to counter cyber threats. According to the respondents, the leadership guiding policy was issued to be prepared and to build a resilient system. The understanding of this policy suggests that the tasks of the operational and tactical leadership are known, and that senior leadership expects preparedness plans to be carried out.

When asked about the authority currently responsible for cybersecurity strategy, AS2, a senior government official and strategic planner, pointed to the Office of the National Security Adviser as the authority responsible for the design of a strategy for cybersecurity and counterterrorism in Nigeria. AS14 explained that the strategy is more about prevention and promotion of interagency collaboration to enhance security through an integrated approach to national risk management. AS8, AS9, AS10, AS13, AS14, and AS15, all from police, intelligence, military, and academia pointed to the fact that the

Nigerian cybersecurity strategy is handled by the president under the Office of the National Security Adviser. AS15 gave me a hard copy of the published document.

Issues of privacy and civil liberties.

Experts raised a constitutional issue in the effort of preventing terrorist networking and expansion in cyberspace: protecting individual privacy and civil liberties. Nigerians conceived the constitution to preserve individual freedoms and liberties. All the participants argued that Nigeria's experience with these issues is different from that of the United States, for example, where the justice system is highly developed. Terrorists and others who use new media technology to spread violence should not enjoy any protections that modern society offers. Two of the participants cited the United States of America Patriot Act that provides appropriate tools required to intercept and obstruct terrorism. Majority of the participants mentioned examples of China, Saudi Arabia, and North Korea, where citizens have limited access to the Internet: "…in China, you cannot even get access to everything on Facebook", AS15 stated.

Researcher: what do you think about violations of the fundamental human rights of suspected terrorists' as citizens protected by the constitution?

AS15 underlined that every citizen has rights and enjoys protection under the Nigeria constitution. However, law enforcement does not wait again to investigate after the fact but uses technologies as a proactive measure to collect information in advance. Law enforcement and intelligence agencies in Nigeria have acquired new legal authority to monitor the communications of suspected terrorists on the Internet. Technologies are

used for interception, monitoring, collection and preservation of evidence to prosecute suspected terrorists in courts of law.

AS14 added that with the advent of modern terrorism, law enforcement has a broader scope to extend the dragnet to collect intelligence useful for dismantling terrorist cells and halting the expansion of their ideology. However, the government identified some of the risks which the method of using cybersecurity technologies pose to human rights, including violations of the rights to privacy and freedom of expression. According to the UN Human Rights Charter, privacy, freedom of opinion and speech are recognized as human rights (UN, 2013). Therefore, the method and application of technologies are performed to meet the standards of within the democratic society to be seeing legitimate and achieve the security goal. Every Nigerian citizen has access to the Internet and can communicate freely without hindrances except those who are suspected of engaging in criminal or terrorist activities. The tactical intelligence is "target-specific" with individuals put under surveillance when they are suspected of plotting actions detrimental to the state. All the participants expressed fear of the abuse of the policy to spy on innocent citizens, especially those who oppose bad government policy. Three of the participants pointed to the government's monitoring activities of activists and a recent clampdown on some journalists.

Effectiveness and practicality of cybersecurity technologies (Q.2)

The principal finding of this study is that measurement of the effectiveness of particular tools may not provide a holistic view of their performance. However, respondents explained that assessment of efficiency would be the ability of the law

enforcement and intelligence agencies to manage both technology and human assets to achieve security goals. Experts interviewed posited that there is no standalone technology; agencies must develop skills, knowledge, and abilities needed for leadership to make technology effective. Also, respondents explained that the effectiveness of a given technology is measured based on cost and proportionality, including whether or not the technology achieved the expected security goal.

Practicality. Participants interviewed argued that the application of cybersecurity technologies is practical in Nigeria's context where law enforcement and intelligence agencies have acquired new legal powers to use cyber surveillance technologies to monitor potential terrorists' communications.

I asked the following questions to provide the answer to Research Question 2:

1. What kind of technologies have been most useful to lessen terrorist networking in cyberspace?
2. How do you select such technologies, what is your testimony about its effectiveness, and how practical are the techniques without violating civil liberties, privacy, and the fundamental human right to free speech?
3. What impacts do such technologies have on privacy and individual liberties?
4. Is there anything else you would like to tell me?

Terrorist organizations use all sorts of Internet-enabled communication technologies to expand their agenda. Experts interviewed spoke of "tools" identified to be useful, such as communication surveillance technologies, content monitoring tools, and

listening devices such as frequency jammers and interception technologies. Security experts refer to all these equipment as “tools” or “technology”.

AS9: Terrorists take advantage of new media; they use mobile phones to communicate with their members and give them instructions about potential targets. They obtain information on the target by researching the web, newsgroups, open source media, or actively seeking the information through legal means for an illegal purpose.

AS10 (an information security specialist): The use of internet-enabled mobile phone technology is an advantage to Boko Haram. The Internet consists of several networked systems that are managed independently with limited control or oversight. It is cheap and could be used efficiently to spread information.

AS10: “Over 50 million people in Nigeria have access to the internet with their mobile phones. Everybody with a mobile phone has access to Facebook, YouTube, Telegram, and WhatsApp. Negative information easily travels fast through this medium.”

Terrorist groups operating in Nigeria such as Boko Haram are able to reach out to a broad audience and manipulate their target by using instant messaging technology like Telegram, WhatsApp, and Chatrooms, including phones. These web tools enable them to effectively communicate with their members and coordinate attacks.

Boko Haram uses communication technologies, including the social media and mobile phones to organize its activities and send messages to a broader audience. For example, the leadership of the group contact [sic] journalists through a telephone to either contest allegations or claim attacks. They usually post videos showcasing their propaganda to www.youtube.com, where millions of people could access them.

Terrorists use technology and one of the ways to combat their activities is through the expanded use of technology. As technology is advancing, the terrorist organization [sic] are becoming sophisticated and increasingly empowered. Experts chose the technologies and evaluated its [sic] effectiveness based on whether it accomplishes the desired security goals or not.

AS9 (has used mobile phones, frequency jammer, and tracking technology successfully in monitoring terrorist activities): "It is quite effective. We are not only able to intercept their [terrorism] communication, but also, we can trace the action back to them and locate them."

When asked how they select suitable security technologies, only seven out of the fifteen participants were able to provide clear answers; they draw their knowledge from their roles as the first lines of defense in law enforcement, secret service, and the military. AS4, AS5, AS9, AS10, AS14 gave almost similar responses as follows.

A variety of technologies are available for cyber security, depending on the technology used for terrorism activities. For instance, if it is known that terrorists use a mobile phone to communicate, frequency jammer may be appropriate. Also, if the threat actors have posted offensive or violent messages on social media or private websites, in most cases, the choice is to work with the service providers to pull down the offensive communication with the aid of interception technology. AS10 commented that "We understand the threat landscape, and we know the kind of weapons the adversaries use and how they deploy them." All the experts agreed that content monitoring tools and installation of firewalls, coupled with other offensive applications are preventive tools

that have been useful. The preventive techniques, which are synonymous with a hardening of the targets, are part of the government's strategy of passive defense. Content monitoring applications are used to filter terrorist messages before they reach the public. The Nigerian Communications Commission, which is the regulator of the communications industry in Nigeria can mandate all the service providers to implement the security measures that detect and discard terrorist communication before they become public.

AS1 (cybersecurity expert) stated that active defense determines the identity of the attack and initiates a counter attack. Computer-driven surveillance, such as voice and facial recognition with interpretation software application are excellent examples of a dynamic defense method. Technology-driven intelligence gathering approach is practical and less intrusive than traditional forms of surveillance and intervention (AS4, AS5, AS9, AS10, AS14).

Security experts interviewed referred to surveillance technology as "tools" or "assets". They described an asset as any equipment, person, facility or information that has value and is controlled by a government. Intelligence agencies such as the Department of State Security Services, Nigeria Intelligence Agency, Directorate of Defense Intelligence and the Office of the National Security Adviser coordinate and deploy various assets to gather intelligence in cyberspace to support counterterrorism operation. The importance of using intelligence tools is to gain advance knowledge of terrorist activities and dismantle their plan before an event occurs. In this context, the categories of surveillance technology identified are a range of technologies such as

listening devices. Also, it includes a frequency tracker, phone jamming tools, which monitor mobile phone calls, and content monitoring tools, which include emails and Internet activities.

Furthermore, identification and authentication technology can reveal who used a computer or a phone to do what, including the location of the users. The question of non-repudiation can further be resolved through a legal process. Also, the use of cryptographic technology for secured communication among law enforcement agents and intelligence and key stakeholders are the best options to avoid information leakages to terrorists and other bad actors.

Overall, the experts viewed the Nigerian government as proactive about ensuring that all mobile SIM cards in Nigeria are registered. All the mobile phone companies operating in Nigeria are compelled to capture biometric features of their customers. The service providers can tell who is doing what with or using his/her mobile phone. Also, they have to cooperate with the law enforcement agencies by providing all the information, such as call logs and information trails when necessary. For instance, the Chinese government has initiated a similar partnership with technology companies as a proactive measure. Kumar (2018) points out that China enacted a National Security Law that gives police the authority to partner with private technology companies to help them bypass encryption or other security tools to access sensitive personal data such as users' emails, text messages, pictures, and the encryption keys that protect them. Giant technology companies like Apple are collaborating with the Chinese government to provide help when needed. Although this approach is raising significant privacy concerns

among users and human right activists, the benefits outweigh the risks if the government is determined to combat terrorism in cyberspace. Meanwhile, law enforcement agents or investigators require a warrant or court order to obtain such information. There are regulations and guidelines for obtaining citizens' information to avoid the abuse of such powers.

AS2, AS4, and AS9 support the notion that new media is a significant advantage to Boko Haram in Nigeria because it helps them keep their activities going while they remain elusive. The opportunity is out there already with the increasing sophistication in communication technologies. It is not possible for the authorities to deny bad actors access to internet infrastructures. However, the authorities can use cybersecurity technologies to thwart terrorists' communication and expansion in cyberspace.

With the evolution of artificial intelligence, there will be no more havens for terrorists operating in cyberspace. AS1 who is a cybersecurity researcher with a private firm corroborated other participants views that the anonymity that cyber actors enjoy is an advantage. However, with artificial intelligence it is possible for security administrators to identify perpetrators and even block messages before they become public. Also, the ability to trace activities back to the offenders with modern digital forensic tools is an added advantage, which AS15 pointed out.

Meanwhile, all the participants pointed to lack of expertise within the intelligence and law enforcement agencies to apply the technologies effectively. According to AS13, "while technology is good and effective, the authorities lacks the expertise to deploy them effectively".

As discussed earlier, one of the primary focuses of the Office of the National Security Adviser is institutional capacity building that includes facilities and human capacity. AS6 said the government should engage indigenous technology companies and encourage research that can produce technologies that target adversaries based on the local threat landscape. At present, there is an apparent lack of confidence in locally made security solutions. The interpretation of these comments agreed upon by all participants indicate that the authority relies more on foreign experts and technologies.

However, two dissenting voices posited that cybersecurity technologies are not a total panacea, but that the long-term strategy should be based on an educational program, deepening democratic culture, alleviating poverty, and expansion of opportunities for young people. AS10, who is a counterterrorism expert supported the notion raised by the two academic professors AS15 and AS12. The implication and interpretation are that technology alone cannot be used to fight terrorism and secure cyberspace. Their use must be comprehensive and accompanied by other social strategies, which include education and awareness programs.

The security experts explained that the effectiveness of technologies is measured based on its technical capability to achieve the security goals. Cayford & Pieters (2018) point out that effectiveness is an impact that is desirable and recognized as contributing towards sought-after security goals. Also, experts viewed the efficiency of cybersecurity technologies from the point of cost-benefit analysis. The justification is that the application of cybersecurity technologies is cheaper and easy to deploy compared with using human assets to perform the same function. Therefore, a risk assessment will

enable a user to gauge the cost of security measures against the threat landscape and apply the best method. It is essential that the benefit of the outcome of the possible actions outweigh the risk to make it useful. All the experts interviewed pointed to the fact that technologies were helpful in the prevention and detection of several online attacks, especially the blocking and removal of terrorist contents before they reach mass audiences. They argue that the enormous spending on building infrastructures and training to support the use of technologies to combat cyberterrorism in Nigeria cyberspace is reasonable and the outcome is desirable.

I posed similar follow-up questions to all the participants since they all considered technology is effective and a practical approach to diminish the effect of the expansionist terrorist program in Nigerian cyberspace. They all clarified that there must be an overall strategy which focuses on targeting the population of young people. All the participants traced the origin of terrorism in their present domain to poverty, inequality, and the lack of opportunity in northeast Nigeria where Boko Haram emerged. They all pointed out that good governance and the deepening of democracies that create room for freedom of expression and broader participation, including the expansion of opportunities for the young people, will lessen the effect of terrorism in cyberspace. It will serve as a long-term solution to the ideology of terrorism if the police, military, and other actors charged with protection reduce the incidence of extra-judicial murder and embrace respect for the rule of law, AS12 stated.

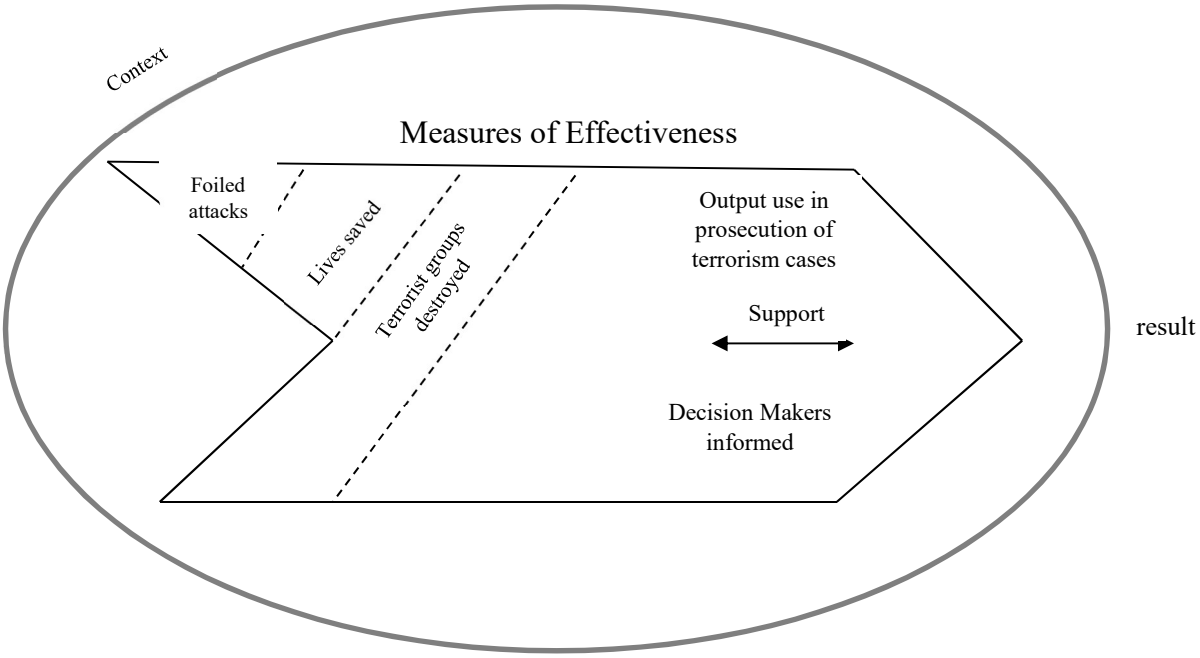

Figure 6. Evaluating the effectiveness of cybersecurity technologies as described by security experts.

Additional measures. On extra measures and policies that the government could implement to incorporate best practices into how to use technologies against adversaries, most participants recommended that Nigeria should embrace the United States' approach. Also, there is an apparent lack of coordination among government agencies. All the participants expressed a valid concern about the disconnection between the law enforcement, intelligence, and government leaders. The Department of State's publication corroborates this fact that interagency cooperation and information sharing in Nigeria are weak and have at times hindered overall effectiveness (United States Department of State, 2017).

First, Nigeria must reaffirm its rights to protect its information space from disturbance from terrorist or nation-state actors. Also, to inspire all sectors, both public and private, including individual citizens to understand their role and responsibilities with

regards to online security, people must be made to understand the threats and prepare to respond to them. Table 5 summarizes the themes uncovered from the interviews with the experts.

Table 5

Themes of Perceived Risk and Counter Risk Measures

Strategic Measure	Operational measure	Tactical measure
Law and Policy	Creating new agencies with focus on countering terrorist propaganda	Human asset-skillful personnel
Cyber Strategies and Capabilities -Building Infrastructures	Active defense with intelligence-driven technologies	Cybersecurity technologies-tools and equipment
International Cooperation	Information database	Funding
Governance of Cyberspace	Private security firm	Awareness
Research		
Preparation – Passive defense- Target hardening	Coordination	
Funding		

Debate raised on the meaning of cyberterrorism. An unanswered question emerged from the interviews on the definition of terrorism. There is some variance in response to interview questions and the most noticeable one is on the definition of cyberterrorism. Some of the participants thought that cyberterrorism and cybercrime connote the same thing. A discrepancy worthy of mention is that the terms "cyberterrorism" and "cybercrime" were used interchangeably by participants. Terrorists

may engage in the act of cyberterrorism to expand their agenda, but may not necessarily cause physical harm. Meanwhile, according to the literature and a majority of the participants, terrorists and criminals may engage in cybercrime such as identity theft, fraud, and money laundering to raise money for their operations. Cyberterrorists pursue their targets using the opportunity the Internet has provided them to expand their ideology. They have the means or capability to operate in cyberspace and the motive is either politics, religion, vendetta, a social cause or a symbolic act. The intention is always to influence an audience or to intimidate the government to accept their demands.

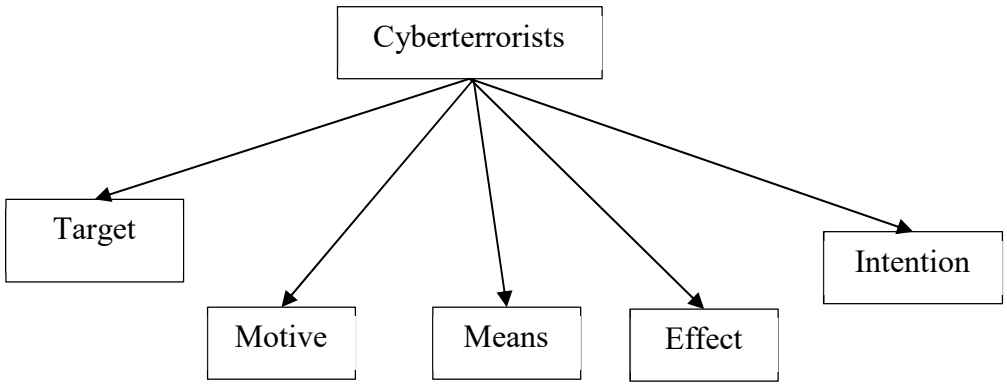

Figure 7. How cyberterrorism is observed by experts.

Summary

In Chapter 4, I presented research questions of this study by data collection, analysis, and results. In Research Question 1, I performed a qualitative interview with security experts, including document content analysis of laws, policies, cybersecurity directives and high-level government declarations. The findings revealed that the integration of technology in counterterrorism strategy creates a new opportunity to develop new technologies and technical skills. Emerging technologies such as artificial intelligence and machine learning algorithm are pointers to the future possibilities of combating enemies in the cyberspace. Technologies remain viable instruments to subdue terrorists' influence in cyberspace. The technological approach is a top priority for law enforcement and intelligence communities. The study findings provide insights into the application of a combination of strategies in support of technology to secure Nigerian cyberspace. Nigeria's national policy on cybersecurity is a guiding document for intelligence organizations, law enforcement agencies, and other security apparatuses in Nigeria.

In Research Question 2, I conducted interviews with security experts, including document content analysis of threat assessment documents, policy, and peer-reviewed literature. The findings revealed that the effectiveness of technologies is measured based on its technical capability to achieve the security goals. Experts clarified that technologies are selected based on risks and must be combined with other strategies to make a good result. Content monitoring tools, firewalls, and identification and authentication tools that guarantee non-repudiation and other technology-driven

intelligence gathering tools have been useful. A combination of surveillance and interception technologies are considered effective based on the numbers of attacks thwarted by the Nigerian Secret Police. Findings on the practicality of the application of the technologies reveal that law enforcement and intelligence agencies have acquired new legal powers to use cyber surveillance technologies to monitor potential terrorists' communications. Therefore, the use of technology is feasible in all situations as it is known to be less intrusive and regulated by law against abuse.

Based on the findings discussed in this chapter, some recommendations are discussed in Chapter 5 with a focus on how to advance the efforts to mitigate the expansion and organization of terrorism in cyberspace. I will also indicate additional areas for investigation which will further improve the security of nations and individuals seeking to benefit from opportunities available in an interconnected world.

Chapter 5: Summary, Recommendations, and Conclusions

Introduction

The Nigeria government has spent billions of dollars to protect its cyberspace, including telecommunication infrastructures from terrorist attack. Also, the government has given considerable attention to cybercrimes such as terrorists' online financing and fundraising activities. However, these efforts have failed to recognize the threats presented by terrorist propagandas in Nigerian cyberspace.

The purpose in this qualitative interview study was to gain an understanding of how experts and security administrators choose cybersecurity technologies to mitigate terrorist propaganda and networking in Nigerian cyberspace. I used qualitative interview study methodology to explore expert perspectives on the role of technology in fighting the expansion and organization of terrorism in cyberspace. This study was qualitative in nature. I used Cohen and Felson's (1979) routine activity theoretical framework to examine existing documents as well as face-to-face interviews with security experts.

Key findings of this study are as follows: that technology is useful in fighting the expansion and coordination of terrorism in cyberspace when properly integrated with other strategies. There has been little progress in countering the threat presented by terrorists' propaganda in Nigerian cyberspace; a need exists to train and produce more experts with the requisite technical skills to dismantle terrorists' websites and counter their messaging on social media platforms; and the government's counter-narrative efforts on social media are ineffective. Cybersecurity technologies are useful and cost-effective tools to combat terrorist propagandas and networking in cyberspace. New

artificial intelligence and machine learning tools enable prominent social media organizations to take down terrorist content faster than human moderators. Nigeria constitution guarantees no protection for people spreading violence and hate speech in cyberspace. Law enforcement and intelligence agencies have inherent powers to listen to citizens' communications, break offenders' privacy, and collect evidence that can stop potential terrorist acts. The government of Nigeria is coordinating with the United States and other western allies in the areas of training and technology transfer.

Interpretation of Findings

Advancements in new information and communication technologies show that terrorist organizations would always take advantage of the media to propagate their violent ideologies because of the level of anonymity the platform provides them. With a RAT theoretical framework, the new media technology is an opportunity for the terrorist organization, and the environment is suitable because of the high reliance on the Internet technology. Waltzman (2017) argued that application of technologies is capable of altering the convergence of the three factors that can make a crime to occur. Therefore, the role of technologies is essential in the prevention of criminal and terrorist activities and the protection of the cyberspace.

For instance, the DSS foiled Boko Haram/ISWAP's attempt to kidnap women in northeastern Nigeria on several occasions with the aid of interception technologies. Internet filtering tools were used successfully to intercept ISWAP communication and to pull down their propaganda messages on social media platforms. The law enforcement agencies have on several occasions removed terrorist content that could have caused a

psychological impact on the targeted population. Internet filtering technologies are capable of conducting automated monitoring of online media sources, including social media sites, websites, blogs, and email. Also, it is capable of suppressing text, images, networks, protocols, and malicious activities (United Nations, 2013). The success stories are evidence that technologies are essential to keeping Nigeria safe and preventing the expansion of terrorism in cyberspace.

Terrorist messages were flagged before getting to the broader audience while techniques were instrumental to the tracking and arrest of offenders. The overall goal of the government is to deploy AI to patrol cyberspace for intelligence gathering and to aid quick response. A key measure of the effectiveness of technologies arises from the number of lives saved based on intelligence collected through those tools to foil terrorists' plans and recruitment agendas in cyberspace. Also, a drone was used successfully as one of the cyber technologies to detect the location of the schoolgirls kidnapped by the terrorist group inside the expansive Sambisa Forest of Nigeria.

In the literature review in Chapter 2, I cited research that indicated that 21st-century terrorists would be sophisticated with the capability to use media technologies to cause extreme damage (Minei & Matusitz, 2012). I was able to confirm these findings based on expert opinions and evidence from the documents reviewed. For instance, terrorists operating in Nigeria are becoming more familiar with new technology. A new generation of more computer-savvy terrorists is growing and focused on using new ICTs to carry out information operations against the public by placing terrorist content such as incitement, misrepresentation, hatred, and violence.

Also, the number of Internet users in Nigeria is above average and this reliance makes most citizens vulnerable to terrorist content. The spreading of messages of violence, fear, and threat entails grave risks to citizens and the society at large. Denning (2000) posits that vulnerability requires some reliance on IT infrastructures.

The predominant theme from findings indicates that experts recognize that cybersecurity technologies, including a set of operational measures, are useful for mitigating the threat of terrorist expansion agenda in Nigeria cyberspace. The literature review presented in Chapter 2 presented a variety of approaches, including content and communication-based responses, to counter the use of cyberspace for violent extremism and terrorist purposes. Berger (2015) suggested that the future of fighting the organization of terrorism in cyberspace will rely on technologies and how they are deployed. The study confirmed, based on experts' opinions, that cybersecurity technologies are valuable to prevent, detect, and deter terrorists in cyberspace.

The government of Nigeria has adopted a technology-neutral approach, which is a form of regulatory process that prevents service providers from preferring one type of technology over another in the provisioning of their services. The results of these study are consistent with Berger's (2015) findings of robust technology as one of the measures to tackle terrorist incursions in cyberspace. The content monitoring tools are proactive and reactive. It enables security to remove the terrorist material before it reaches the public domain. It is the best and most successful tool against enemies in cyberspace. It enables security agents to gather more intelligence about the actors through the analysis of their messages. With this, the authority can have clear pictures of who they are and

their mission. A proper review of their messages could help to distinguish between hacktivists and cyber terrorists through adequate identification of threat actors' intentions. The government can initiate a social approach to alleviate the threat or start a dialogue with the actors when necessary. Also, it enables law enforcement agents to identify the origin and trace the crime back to the threat actors through digital forensics analysis.

The law enforcement and intelligence agencies collaborate with technology and communication companies to suspend jihadist accounts and remove their messages so as to reduce the effect before it diffuses to the entire online community. Government stakeholders and security experts know that terrorist organizations seek to exploit the opportunity of the interconnectivity of cyberspace. For this reason, making terrorists' messages harder to access may reduce their activities and lessen the effect of their radical ideological propagation on target populations. Nigeria lacks a formal policy, which has inhibited both the government and the private sector from implementing coordinated procedures and programs to address the weaknesses in their responses. The study allowed me to investigate the multiple organizations responsible for protecting and enforcing the law in Nigerian cyberspace. The need exist for active cooperation and interagency interaction to strengthen the attack method against the adversaries. The findings of this study are consistent with Osho and Onoja's (2015) conclusions that domestic and international alliances are a crucial aspect that must be integrated into the overall strategy. This approach should involve consistent intelligence sharing and technology transfer, which must be initiated by the appropriate authorities. Partnership with the

private sector is vital because private organizations manage approximately 90% of the communication infrastructures while the government only regulates their affairs. For instance, Facebook, Twitter, WhatsApp and mobile phones are owned by private sectors. Therefore, they remain the first line of defense and will continue to play a crucial role in protecting and managing the information that goes to the public. The need exists for a strong partnership between technology companies and the government to combat terrorism in Nigerian cyberspace. This result is aligned with the work of Al Mazari et al. (2016) on the need for coordination among national military and law enforcement agencies and civilians.

Moreover, no public education program to inform the Nigerian public about the risks in the cyber environment. The mobile Internet applications, which are most accessible to the population via smartphones particularly increase the risks and could inhibit the country from achieving the full benefits of an interconnected economy. Liang (2015) argued that countering the strength of terrorist recruitment and influence must be based on building resilience among populations vulnerable to radicalization.

In Chapter 2, Flashpoint (2016) posited that cyber terrorists use social media to communicate with one another and the entire world because of the borderless nature of cyberspace. I found out in the course of my study that ISIS uploads most of the propaganda content for Boko Haram from outside Nigeria. Because cyberterrorists can upload their content from anywhere, the source of such violent information or propaganda does not necessarily have to be a country with a high level of technological development. Hence, it is essential for the Nigerian government to ally with many

countries with different backgrounds. Therefore, I fully emphasizes the importance of cooperation in response to the threats coming from cyberspace.

I chose Cohen and Felson's (1979) routine activity theoretical (RAT) framework for the study. Security response to the terrorist activities in cyberspace can easily be understood in RAT terms. Nigeria's government can adopt and implement a law that empowers security agencies to use technologies to prevent and counter violent extremism broadly. Making it harder for terrorists to place content on online platforms by using new artificial intelligence and machine learning tools to take down their messages will frustrate them and decrease their motivation. The study established the veracity of this notion based on experts' perceptions of the effectiveness of cybersecurity technologies and their practicality.

Moreover, there is a lack of awareness on the part of public and government, and a failure to recognize the fact that the methods of countering terrorist activities in cyberspace are improving in tandem with the level of sophistication of their tactics and weapons. This failure is a significant source of vulnerability to cyberterrorism. Therefore, increased awareness on the part of the public and private sectors could help to raise the level of cooperation among law enforcement and technology companies. Overall, awareness of the risk will help to reduce vulnerability.

By analyzing and understanding the threat posed by terrorist propaganda in cyberspace to the public and entire national security of a nation, as well as the commerce that these facilities support, the findings of this study advance knowledge in the discipline of homeland security based on its exploration of logical questions related to this threat.

Moreover, this study's results extended disciplinary knowledge found in the peer-reviewed literature described in Chapter 2, specifically in the thematic areas contained within counterterrorism, national security, and cybersecurity.

Based on experts' opinions, the organization and expansion of terrorism in cyberspace is divided into three categories, which are: disruptive and destructive information attacks, facilitation of technology to support an ideology, and communication, fundraising, recruitment, and propaganda. The analysis revealed an overlap between cybercrime techniques and cyberterrorism. The government is persuaded to adopt and implement measures and to develop the capability to prevent and counter violent extremism and terrorism in the cyberspace. These methods should comply with Nigeria's obligations under international law and respect for the applicable law under the constitution.

The Global Counterterrorism Working Group (as cited in GCTF, 2017) states that it is essential for the government to recognize the role of ICT and technology companies as regards the availability and accessibility of terrorist content online. My study has confirmed that law enforcement and intelligence agencies are helpless without the full cooperation of the technology companies.

Finally, the study confirms that weak leadership, nepotism, corruption, and lack of technological know-how continue to plague the agencies responsible for security in Nigeria. Political instability, ethnic and religious influence, and inefficiency are compounding the potential vulnerabilities to terrorism. Terrorist organizations in Nigeria will recruit more "lone wolf" attackers, including suicide bombers in cyberspace. Boko

Haram/ISIS are frequently using encryption technology to communicate unnoticed, including the dark web, and cryptocurrencies to recruit new members and spread propaganda. Given the level of increasing sophistication of cyber capabilities of young people in Nigeria, it would be easy in future to acquire a capacity to make weapons of mass destruction that can facilitate their operations, including weapons to conduct physical attacks against targets. Given the level of poverty, government repression, and lack of opportunities for young people, the country is a fertile ground for terrorist recruitment. In future, terrorists and armed groups in Nigeria will attack critical infrastructures, including financial and aviation systems, using cyberspace. It is just a matter of when it will happen, hence the need for adequate response.

Limitations of the Study

As a qualitative interview study, the research is limited in scope and the duration of the field work was May through June 2018. As I noted in Chapter 4, better and richer data was obtained during face-to-face interviews. However, the study could only exploit publicly available open-source data and was unable to use documents which are classified in nature. This limitation precluded the examination of security documents related to terrorist campaigns or intelligence, including material related to criminal activities deemed to unreleasable.

Also, the study involved a limited number of participants which were not selected from every sector of Nigeria. Most operators of non-governmental organizations and activist groups hold strong opinions about privacy and civil liberty concerns as related to the government's cybersecurity program. The groups were not adequately represented in

this study due to the scope of the research and limited resources. This limitation was mitigated as much as possible by interviewing participants from multiple government security agencies along with various representatives from the private sector and academia, but this missing sector should be considered in future studies due to their exposure to risk and diverse experiences and worldviews. The consensus and divergent views of the participants are represented in the discussion in Chapter 4.

Despite this limitation, the results from the study and related interpretations should be used to generate genuine interest and guide studies that examine this potent threat. By using this study's framework and method of gaining experts' perception of the role of cybersecurity technologies in combating the organization and expansion of terrorism in cyberspace, knowledge in the discipline will be advanced. This study acts as a foundation upon which further research can build to advance homeland security.

Recommendations

Research and analysis enable academia to provide innovative thinking and perspectives on threats. Therefore, academia plays a significant role in counterterrorism. Given the strengths and limitations of this study, the following recommendations are presented in two segments. The first part focuses on recommendations to the government of Nigeria as related to the findings, while the second section focuses on areas for future research.

Recommendations for Future Study

First, this research focused on the role of technology in mitigating the expansion of terrorism in cyberspace. There is a need for further quantitative research to measure the effectiveness of cybersecurity technologies in Nigerian cyberspace.

Second, there is a need for research in the area of international law enforcement cooperation on the use of technologies. Future research should include analysis of jurisdictional problems regarding the investigation of acts of terrorism in the West African region. Considering should be given to how law enforcement cooperation should be put into practice. Future studies should focus on how international bodies, such as Interpol, Europol, and other regional training centers facilitate cooperation by examining the principles of those entities and how they implement them.

Third, future research should focus on how terrorist organizations might use ICT infrastructure for prospective attacks after being frustrated out of online platforms. Fourth, given the Russian cyber-operation noticeable in the last US election, this study should be replicated with a focus on information operations by nation-state actors like Russia.

Implications

The findings from this qualitative interview study have contributed to positive social change and thereby to Nigeria's national security by providing data to key stakeholders responsible for decision making and policy formulation regarding cybersecurity, counterterrorism, intelligence operation, and law enforcement. If the insights from this study are incorporated into Nigeria's cyber strategies and capabilities,

they could improve the capacity of the nation to confront a series of threats to its security and simultaneously position itself better to reap the rewards in the form of peace and stability. Also, the study provides impetus that helps the public, law enforcement, and the intelligence community to build capacity using relevant cybersecurity technologies to confront a series of cyber threats, especially the organization and expansion of terrorism in cyberspace.

Due to societal reliance on ICT infrastructures, the security of cyberspace is essential and a significant concern for Nigeria and the world at large. The insights from this study will enable the government of Nigeria to develop counterterrorism measures that will deny terrorists cyber sanctuary, including the elimination of terrorist resources that allow the group to spread propaganda as well as conduct cyber mobilization and recruitment. Moreover, the creation of a secure environment, including comprehensive and integrated information operations are critical factors to consider for counterterrorism operations.

As highlighted in the Nigeria National Cybersecurity Strategy, the country is currently looking to build trust in the ICT sectors so as to facilitate economic growth, diversity, and youth employment creation (ONSA, 2014). A long-term strategy of building institutional capacity and fostering intellectual human capital, which has been pointed out in this study, will add to national growth and positive social change.

Recommendations for the government of Nigeria

First, based on the assessment of Research Question 1, technology is significant in fighting the expansion and organization of terrorism in cyberspace. As part of a long-term

strategy, the government of Nigeria must work with the ministry of education in Nigeria to develop curricula to groom future cyber experts. This step will create expertise and inspire students to pursue the profession. Technology is a national security tool. Hence, Nigeria's cyber-capabilities must be established and well documented.

Collaboration is essential in the fight against the organization and expansion of terrorism in cyberspace. As recommended in the Country Report 2016 released by the US Department of State, it is essential for Nigeria's government to strengthen its bilateral and multilateral relationships (United States Department of State, 2017). Such ties will facilitate technology transfer and information sharing among ally states and partners. Cooperation and training to prepare for contingencies is the only proper way to guarantee results in the event of a terrorist emergency.

Also, there is a need to create a military cyber command or an agency that will mirror the United State Defense Advanced Research Projects Agency (DARPA). While a cyber command would safeguard information security in the armed forces and across the entire infrastructure of Nigeria, a similar agency to DARPA would focus on developing emerging technologies for use by the military. The agency will facilitate technological research, including capacity building to train people and create varieties of software that will enable the government to develop a centralized protection system shielding.

Public partnerships and industry alliances are critical for technology and human development. Nigeria's government should implement a series of information security measures based on a public-private partnership strategy in order to overcome the technological lag in its cybersecurity science. Further, it is essential to strengthen the

criminal justice system with a focus on prioritizing how to investigate and prosecute suspected terrorism cases.

Finally, there is a need to commit to the rule of law. It is essential to establish and maintain international standards of accountability. Commitment to the rule of law is highly crucial in the war against terrorism. When confronting terrorism, democratic governments must recognize not only whom they are fighting, but also the basis of the fight. Therefore, when a government does not adhere to its laws, terrorists use it as propaganda against the government. The public must see actions to combat terrorism as being legal in order to warrant public support.

Conclusions

Emerging technologies play an essential role in countering the expansion and organization of terrorism in cyberspace. The study's findings suggest that the application of technologies would be a solution to combat cyberterrorism activities. Terrorist organizations have shifted the battleground to cyberspace because it is a cheap alternative to communicate and coordinate activities with a high level of anonymity. Boko Haram and other terrorist groups operating from Nigeria have used cyberspace to talk to the world, sending fearful content, incitement, and violent messages.

The technological approach complemented with other strategies is the future of the fight against the expansion of extremist ideology, mobilization, coordination, and terrorist influence in cyberspace. For instance, technologies such as artificial intelligence are crucial and will have enormous impact and boost counterterrorism efforts. As such,

the role of cybersecurity technologies in tackling myriad cyberthreats, including terrorists' activities in online platforms cannot be overemphasized.

The results of this study provide insights into the national development of cyber strategy and capability process in Nigeria. The qualitative interview study methodology proved to be appropriate at this point in Nigeria because of the ongoing efforts to secure the nation's cyberspace from being entirely hijacked by terrorists. The results of this study provide insights that deepen understanding of the role of technologies in combating the expansion of terrorism in Nigerian cyberspace. The findings reveal that technologies are useful for cyberspace patrol, surveillance, intelligence gathering, and prevention. Technologies are selected based on the risks and must be tailored towards deterrence, detection, prevention, and response. The findings confirm that the issue of civil liberty is better overcome when the technological strategy is combined with other strategies, including regulation, law, and procedures.

The study identified the importance of international cooperation and proposed that the Nigerian government strengthen its bilateral and multilateral cooperation. International collaboration will facilitate technology transfer, training, funding assistance, and information sharing. Nigeria should establish a standard in line with international laws while dealing with the issue of terrorism.

In the hope of contributing to positive social change by improving the security of Nigerian cyberspace, I explored security experts' perspectives on the role of cybersecurity technologies in fighting the expansion of terrorism in cyberspace, including the effectiveness and how it is deployed. I made recommendations based on my findings,

to be implemented by stakeholders in public and private sectors. Also, additional future research was recommended in Chapter 5 to improve the security of Nigerian cyberspace.

References

Abrahms, M., & Conrad, J. (2017). The strategic logic of credit claiming: A new theory for anonymous terrorist attacks. *Security Studies,* 26(2), 279–304. doi:org.ezp.waldenulibrary.org/10.1080/09636412.2017.1280304

Adomi, E. E., & Igun, S. E. (2008). Combating cybercrime in Nigeria. *The Electronic Library,* 26(5), 716–725. doi: http://dx.doi.org/10.1108/02640470810910738

Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2016). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. *International Journal of Cyber Warfare and Terrorism,* 6(1), 1–12. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=108722952&site=eds-live&scope=site

Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2017). Introduction to the special issue: Terrorist online propaganda and radicalization. *Studies in Conflict & Terrorism*, 40(1), 1–9. doi:10.1080/1057610X.2016.1157402

Allision, M., Anne, S., & Ahmet S., Y. (2017). Beating ISIS in the digital space: Focus testing ISIS defector counter-narrative videos with American college students. *Journal for Deradicalization,* Vol Spring, Iss 10*,* 50–76 (2017), (10), 50. Retrieved from http://journals.sfu.ca/jd/index.php/jd/article/view/83/73

Barnes, J. E., Fidler, S., Lubold, G., & Shishkin, P. (2015, Nov 21). The war on the Islamic state: To prevail, west must settle on military tactics, cut off oil money, counter propaganda, strategists say. *Wall Street Journal*. Retrieved from

https://search-proquest-com.ezp.waldenulibrary.org/docview/1735319573?accountid=14872

Barlow, J. P. (1996). A declaration of the independence of cyberspace in J. Casimir (ed.) Postcards from the Net: *An Intrepid Guide to the Wired World*, pp. 365–367. Sydney, Australia: Allen and Unwin.

Baken, D. (2013). Cyber warfare and Nigeria's vulnerability. *E-International Relations, 3.* Retrieved from http://www.e-ir.info/2013/11/03/cyber-warfare-and-nigerias-vulnerability/

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *Qualitative Report*, *13*(4), 544–559. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=37243095&site=eds-live&scope=site

Benson, D. C. (2014). Why the internet is not increasing terrorism. *Security Studies*, 23(2), 293–328. https://doi-org.ezp.waldenulibrary.org/10.1080/09636412.2014.905353

Berger, J. M. (2015). The evolution of terrorist propaganda: The Paris attack and social media. Retrieved from http://docs.house.gov/meetings/FA/FA18/20150127/102855/HHRG-114-FA18-Transcript-20150127.pdf

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of*

Cyber Criminology, 3(1), 400 –420. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=52650847&site=eds-live&scope=site

Boyce, C., & Neale, P. (2006). Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input. Watertown, MA *Pathfinder International.* Retrieved from https://dmeforpeace.org/sites/default/files/Boyce_In%20Depth%20Interviews.pdf

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, 9(2), 27–40. https://doi-org.ezp.waldenulibrary.org/10.3316/QRJ0902027

Cayford, M., & Pieters, W. (2018). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, 34(2), 88–103. https://doi-org.ezp.waldenulibrary.org/10.1080/01972243.2017.1414721

Che, E. (2007). Securing a network society cyber-terrorism, international cooperation and transnational surveillance. *Research Institute for European and American Studies* Research Paper No, 113.

Chu, H. C., Deng, D. J., Chao, H. C., & Huang, Y. M. (2009). Next generation of terrorism: Ubiquitous cyber terrorism with the accumulation of all intangible fears. *J. UCS*, 15(12), 2373–2386. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000273177200006&site=eds-live&scope=site

CIA (2017). The world factbook: Nigeria. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/ni.html

CNN. (2015, January 12). CENTCOM Twitter account hacked, suspended – *CNN Politics.* Retrieved from http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/index.html

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588–608. Retrieved from http://www.personal.psu.edu/users/e/x/exs44/597b-Comm%26Crime/Cohen_FelsonRoutine-Activities.pdf

Conway, M. (2002). Reality bytes: Cyberterrorism and terrorist 'use' of the Internet. *First Monday*, *7*(11). Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=conedsqd6&AN=edsair.od.....119..1adb6237029a4fd3e6efc42e0a68a250&site=eds-live&scope=site

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719–731. https://doi-org.ezp.waldenulibrary.org/10.1016/j.cose.2011.08.004

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1), 308. Retrieved from https://ezp.waldenulibrary.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=36133473&site=eds-live&scope=site.

Cordesman, A. H., & Cordesman, J. G. (2002). Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland. *Greenwood Publishing Group.*

DCSINT (2006). Critical infrastructure threats and terrorism. Retrieved from https://rdl.train.army.mil/catalog-ws/view/100.ATSC/898B610C-E6C9-4CF9-B6D4-7278BB558772-1302982125245/dcsint_hdbk1/dcsint_hdbk_1.02.pdf

Dean, G., Bell, P., & Newman, J. (2012). The dark side of social media: review of online terrorism. *Pakistan Journal of Criminology*, 3(3), 103–122.

Denning, D. (2000, August 24). Cyberterrorism. Retrieved from http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf

Edwards, R., & Holland, J. (2013). What is qualitative interviewing? *A&C Black.*

Falessi, N., Gavrila, R., Klenstrup, M.R., & Moulinos, K. (2012). National cyber security strategies: Practical guide on development and execution. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Fink, E., Pagliery, J., & Segall, L. (2015, November 24). Technology and the fight against terrorism. *CNN Tech*. Retrieved from http://money.cnn.com/2015/11/24/technology/targeting-terror-intelligence-isis/index.html

Flashpoint. (2016, July 22). Flashpoint's new research illuminate's jihadists' digital toolbox. Retrieved from https://www.flashpoint-intel.com/press-post/flashpoints-new-research-illuminates-jihadists-digital-toolbox/

Foley, F. (2009). Reforming Counterterrorism: Institutions and Organizational Routines in Britain and France. *Security Studies,* 18(3), 435–478. doi:10.1080/09636410903132920

GCTF. (2015, September 15). Countering violent extremism: Zurich-London recommendations on preventing and countering violent extremism and terrorism online. Global Counterterrorism Forum. Retrieved from https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/A/GCTF%20-%20Zurich-London%20Recommendations%20ENG.pdf?ver=2017-09-15-210859-467

Gelo, O., Braakmann, D., & Benetka, G. (2008). Quantitative and qualitative research: Beyond the debate. *Integrative Psychological & Behavioral Science,* 42(3), 266–290. doi:10.1007/s12124-008-9078-3

Glenn A., B. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal,* (2), 27. doi:10.3316/QRJ0902027

Global terrorism index. (2016). Measuring and understanding the impact of terrorism. Sydney, Australia: *Institute for Economics and Peace*. Retrieved from http://economicsandpeace.org/wp-content/uploads/2016/11/Global-Terrorism-Index-2016.2.pdf

Goduka, N. (2012). From positivism to indigenous science: A reflection on world views, paradigms and philosophical assumptions. *Africa Insight*, *41*(4), 123–138.

Goldman, J. (2011). Words of intelligence: an intelligence professional's lexicon for domestic and foreign threats (Vol. 14). *Scarecrow Press*.

Goodman, S. E. (2007). Cyberterrorism and security measures. Kumar, Arvind et al, eds, 43–54.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies,* 10(2), 243–249.

Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010). Leaving deterrence behind: War-fighting and national cybersecurity. *Journal of Homeland Security & Emergency Management*, *7*(1), 1–24.

Harknett, R J., & Stever, J. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management, 6* (1), Article 79. doi: 10.2202/1547-7355.1649

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, *71*(3), 455–460. doi:http://dx.doi.org.ezp.waldenulibrary.org/10.1111/j.1540-6210.2011.02366.x

Henwood, K. (2014). Qualitative research. *Encyclopedia of Critical Psychology*, 1611–1614.

Hinnen, T. M. (2004). The cyber-front in the war on terrorism: Curbing terrorist use of the Internet. *The Columbia Science and Technology Law Review*, *5*(5), 1–42.

Hoffman, B. (2016). The global terror threat and counterterrorism challenges facing the next administration. *CTC Sentinel*, *9*(11), 1–8.

Hoffman, B. (2016). The coming ISIS–al Qaeda merger. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/2016-03-29/coming-isis-al-qaeda-merger

Holt, T, (2016, April). How terrorist groups use technology to recruit members - *Business Insider.* Retrieved from http://www.businessinsider.com/heres-how-terrorist-groups-use-technology-to-recruit-new-members-2016-4

Homeland Security News Wire (2017 August 22). Encrypted app allows extremists to plot attacks without detection. Retrieved from http://www.homelandsecuritynewswire.com/dr20170809-encrypted-app-allows-extremists-to-plot-attacks-without-detection

Isaac, M. (2016, December 6). Facebook and other tech companies seek to curb the flow of terrorist content. *New York Times.* p. B4.

Kaplan, E. (2009). Terrorists and the Internet. *Council on Foreign Relations*, 8.

Kaplan, J., Lööw, H., & Malkki, L. (2014). Introduction to the special issue on lone wolf and autonomous cell terrorism. *Terrorism and Political Violence*, *26*(1), –12. doi.org.ezp.waldenulibrary.org/10.1080/09546553.2014.854032

Keller, J. (2015). The growing role of technology in the global war on terrorism. Retrieved from https://www.militaryaerospace.com/articles/2015/12/counter-terrorism-technology.html

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, 30(4), 470–486.

Ki-moon, B. (2012). The use of The Internet for Terrorist Purposes. New York: United Nations.

Kim, Y. (2011). The pilot study in qualitative inquiry: Identifying issues and learning lessons for culturally competent research. *Qualitative Social Work*, 10(2), 190–206.

Korolov, M. (2017, October 19). How AI can help you stay ahead of cybersecurity threats. *CSO Online.* Retrieved from https://www.csoonline.com/article/3233951/machine-learning/how-ai-can-help-you-stay-ahead-of-cybersecurity-threats.html

Kumar, M. (2018, July). Apple Transfers Chinese Users' iCloud Data to State-Controlled Data Centers. The Hacker News. Retrieved from https://thehackernews.com/2018/07/apple-china-icloud-data.html

Lee, N. (2015). Artificial Intelligence and data mining. In *Counterterrorism and Cybersecurity* (pp. 323–341). Cham.: Springer.

Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: *Center for Strategic & International Studies.*

Liang, C. S. (2015). Cyber Jihad: Understanding and Countering Islamic State Propaganda.

Luiijf, E., Besseling, K., & Graaf, P. D. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, 9(1), 3–31. doi:10.1504/IJCIS.2013.051608

Lohmann, D. (2016, June 20). How terrorists' use of social media points to the future. Retrieved from http://www.govtech.com/em/safety/Terrorists-And-Social-Media.html

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, 31(5), 381–410.

Maiangwa, B., & Agbiboa, D. (2014). Why Boko Haram kidnaps women and young girls in north-eastern Nigeria. conflict trends, 2014(3), 51–56.

Martin, S., & Weinberg, L. B. (2016). Terrorism in an era of unconventional warfare. *Terrorism and political violence*, 28(2), 236–253.

Mechan, P., and Speier, J. (2011), Boko Haram, threat to the U.S. Homeland. Washington: U.S. House of Representatives Committee on Homeland Security Subcommittee on Counterterrorism and intelligence. National Bureau of Statistics. (2009). *Social Statistics in Nigeria.* Abuja: The NBS Publication.

Minei, E., & Matusitz, J. (2011). Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis. *Journal of Human Behavior in the Social Environment*, 21(8), 995–1019. doi:10.1080/10911359.2011.588569

Minei, E., & Matusitz, J. (2012). Cyberspace as a new arena for terroristic propaganda: an updated examination. Poiesis & Praxis, 9(1–2), 163–176.

Miró, F. (2014). Routine activity theory. The Encyclopedia of Theoretical Criminology.

Musa, A. O. (2012). Socio-economic incentives, new media and the Boko Haram campaign of violence in Northern Nigeria. Journal of African Media Studies, 4(1), 111–124.

Moore, J. (2017, September 7). ISIS supporters call for poisoning of food in grocery stores across U.S. and Europe. *Newsweek.* Retrieved from http://www.newsweek.com/isis-supporters-call-poisoning-grocery-stores-us-and-europe-660750?utm_campaign=NewsweekFacebookSF&utm_source=Facebook&utm_medium=Social

Murrill, R. (2011). The question of cyber terrorism. Forensic Focus. Retrieved from https://articles.forensicfocus.com/2011/07/23/the-question-of-cyber-terrorism/

Ndubueze, P. N., & Igbo, E. U. M. (2013). Third parties and cyber-crime policing in Nigeria: Some reflections. *Policing: A Journal of Policy and Practice*, 8(1), 59–68.

O'Brien, K. (2003). Information age, terrorism and warfare. Small Wars and Insurgencies, 14(1), 183–206.

Ogun, M. N. (2012). Terrorist use of internet: possible suggestions to prevent the usage for terrorist Purposes. *Journal of Applied Security Research*, 7(2), 203–217. doi:10.1080/19361610.2012.656252

Olajide, F., & Adeshakin, K. (2016). Towards the investigation of using social network analysis for counterterrorism in west Africa: case study of Boko Haram in Nigeria. *Journal of Engineering Science and Technology*, 11(11), 1629–1638.

Oluwafemi, O., Adesuyi, F. A., & Shafi'i, M. A. (2013). Combating terrorism with cybersecurity: The Nigerian perspective. World journal of computer application and technology, 1(4), 103–109.

ONSA (2014). National Cybersecurity Policy. Retrieved from https://www2.cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_POLICY.pdf

Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: A qualitative analysis. *International Journal of Cyber Criminology*, 9(1), 120.

Pelfrey, W. V. (2009). An exploratory study of local homeland security preparedness: Findings and implications for future assessments. *Criminal Justice Policy Review,* 20(3), 261–273.

Privacy International. (2018). Video: What is communications surveillance? | *Privacy International*. Retrieved from https://privacyinternational.org/video/1624/video-what-communications-surveillance.

Ranger, S. (2017, August 29). Cyberwar: A guide to the frightening future of online conflict. *ZDNet*. Retrieved from http://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/#ftag=RSSbaffb68

Ravitch, S. M., & Carl, N. M. (2016). *Qualitative research: Bridging the conceptual, theoretical, and methodological.* Thousand Oaks, CA: Sage Publications.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior,* 38(11), 1149–1169.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior*, 38(11), 1149–1169. doi.org/10.1177/0093854811421448

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology,* 11(1), 25–41. doi:10.1080/14780887.2013.801543

Rogan, H. (2006). Jihadism online-A study of how al-Qaeda and radical Islamist groups use the internet for terrorist purposes. *FFI/Report*, 915, 2006.

Rosand, E. (2003). Security council resolution 1373, the counter-terrorism committee, and the fight against terrorism. *American Journal of International Law*, 97(2), 333–341.

Rubin, H. J., & Rubin, I. S. (2012). Qualitative interviewing: The art of hearing data (3rd ed.). *Thousand Oaks,* CA: Sage Publications.

Rudestam, K. E., & Newton, R. R. (2015). Surviving your dissertation: A comprehensive guide to content and process (4th ed.). *Thousand Oaks*, CA: Sage. ISBN: 978-1-4522-6097-6

Sandler, T. (2015). Terrorism and counterterrorism: An overview. *Oxford Economic Papers*, 67(1), 1–20.

Sauter, M., & Carafano, J. J. (2012). Homeland Security: A Complete Guide. *McGraw-Hill.*

Schweitzer, D. (2005). Be prepared for cyberterrorism. *Computerworld*, 39(13), 42.

Schechner, S. (2015, Dec 04). EU presses tech giants in terror fight. *Wall Street Journal.* Retrieved from https://search-proquest-com.ezp.waldenulibrary.org/docview/1738998867?accountid=14872

Schultz, R. (2015, July). Countering extremist groups in cyberspace. *Joint Forces Quarterly,* 79. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_54-56_Schultz.pdf

Simon, M. K. (2011b). Validity and reliability in qualitative studies. In dissertation and scholarly research*: Recipes for success* (pp. 1–3). Seattle, WA: Dissertation Success. Retrieved from http://dissertationrecipes.com/wp-content/uploads/2011/04/Validity-and-Reliability-in-a-Qualitative-Study.pdf

Smith, J. A. (Ed.). (2007). Qualitative psychology*: A practical guide to research methods*. Sage.

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal* (RMIT Training Pty Ltd Trading as RMIT Publishing), 11(2), 63–75. doi:10.3316/QRJ1102063

Thomas, G., Vilmos F., M., & Peer C., F. (2013). Chapter 3 The Two QCAs: From a Small-N to a Large-N Set Theoretic Approach. *Emerald Group Publishing* Limited. doi:10.1108/S0733-558X(2013)0000038007

Tugwell, M. (2017). Terrorism and propaganda: Problem and response. *In Insurgent Terrorism* (pp. 51–61). Routledge.

Turner III, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The qualitative report,* 15(3), 754.

United Nations. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. *Human Rights Council.* Retrieved from https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

United States Department of State Publication (2017, July). Country reports on terrorism 2016. *Bureau of Counterterrorism.* Retrieved from https://www.state.gov/documents/organization/272488.pdf

Waltzman, R. (2017). The weaponization of information. Retrieved from https://www.armed-services.senate.gov/imo/media/doc/Waltzman_04-27-17.pdf

Weeraratne, S. (2017). Theorizing the expansion of the Boko Haram insurgency in Nigeria. *Terrorism and Political Violence*, 29(4), 610–634.

Weimann, G. (2006). Virtual disputes: The use of the internet for terrorist debates. *Studies in conflict & terrorism*, 29(7), 623–639.

Weimann, G. (2014). New terrorism and new media. *Wilson Center Common Labs*, 2, 1–17.

Yin, R. (2009). Case study research: Design and methods (Kindle 4th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Zucker, D. M. (2009). How to do case study research. Retrieved from http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1001&context=nursing_faculty_pubs

Appendix B: Interview Protocol

Interview Protocol

Date: _____

Location: _____

Name of Interviewer: _____

Name of Interviewee: _____

Interview Questions:

1. Let me begin with what you can tell me about the risk associated with terrorist organizations messages of violence, and radical ideology in the cyberspace?

2. What do you see as the role of technology in fighting expansion and organization of terrorism?

3. How would you describe the current level of understanding of this kind of cyber threat by senior government and private sector officials in Nigeria?

4. How would you characterize the ongoing efforts being undertaken to protect Nigerian cyberspace from being entirely hijacked by terrorists to spread a message of violence?

5. What kind of technologies have been most useful to lessen terrorist networking in cyberspace?

6. How do you select such technologies, what is your testimony about its effectiveness, and how practical are these techniques without violating civil liberties, privacy, and the fundamental human right to free speech?

7. What impact do such technologies have on privacy and individual liberties?

8. Which authority/ies is/are responsible for cybersecurity strategy? Where is this determined/published?

9. What additional measures and policies could the government implement to incorporate international best practices into how to use technology against terrorist adversaries?

10. Is there anything else you would like to tell me?