Masthead Logo

Journal of Strategic Security

Volume 12 | Number 1 Article 4

Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies

Sunday O. Ogunlana
Walden University, abovejordan@gmail.com

pp. 72-106

Recommended Citation
Ogunlana, Sunday O.. "Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies." *Journal of Strategic Security* 12, no. 1 (2019): : 72-106.
DOI: https://doi.org/10.5038/1944-0472.12.1.1707
Available at: https://scholarcommons.usf.edu/jss/vol12/iss1/4

Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies

Author Biography

Sunday Oludare Ogunlana, Ph.D., is a counterterrorism policy analyst, and currently a member of the Security Incident Management Team for CitiGroup, as a Senior Security Analyst in Irving, Texas. Previously, he was Group Managing Director of UESIRI Security Service Limited, Abuja, Nigeria. He has served on numerous boards, including Council for African Security Affairs (CASA) and Editorial of African Journal for Counterterrorism. He is the initiator of African Security Forum and Annual Symposium on Counterterrorism that holds at Kofi Annan International Peace Keeping Training Center (KAIPTC) every year. He was Security Advisor to the Chairman of Nigeria Presidential Amnesty Council (PAC) between the year 2012 to 2015.

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 in cyberspace. Using routine activity theory, this article assessed the effectiveness of technological approaches to mitigating the expansion and organization of terrorism in cyberspace. Data collection included open-source documents, government threat assessments, legislation, policy papers, and peer-reviewed academic literature and semistructured interviews with fifteen security experts in Nigeria. The key findings were that the new generation of terrorists who are more technological savvy are growing, cybersecurity technologies are effective, and bilateral/multilateral cooperation is essential to combat the expansion of terrorism in cyberspace. 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 in cyberspace.

Introduction

The Nigeria government has spent a significant amount of money to protect its cyberspace, including telecommunication infrastructures from terrorist attack. In addition, the government has given considerable attention to cybercrimes such as terrorists' online financing and fundraising activities. However, these efforts have in the past failed to recognize the threats presented by terrorist propaganda in Nigerian cyberspace. Cyberspace is increasingly becoming the platform to promote terrorism because it allows easy access to actors to disseminate information beyond geographic borders. The internet and social media create alternative realities for actors, and audiences and users are influenced by the information given to them by strangers.[1] 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.[2] 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, the Nigerian government has just begun to incorporate robust active and passive defense measures against adversaries into the National Security Strategy.[3]

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 in the society. 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. Information communication technology (ICT) is a new tool of attack in the hand of terrorist organizations. Indeed, terrorism is about information. 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.[4]The present danger is that modern-day terrorists have transformed Information communication technology (ICT) 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, drive fundraising efforts, recruitments, and call for terror actions. Kaplan pointed out that terrorist websites moved from fewer than 100 to 4,800 between 2006 and 2008.[5] 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. Therefore, 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. 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.[6] In addition, the literature suggests that the future of fighting extremism, falsehoods, and bogus information in cyberspace depends on the deployment of robust technology.[7] 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 government should use the expertise. Different countries, including Nigeria, used several kinds of technologies to mitigate the effect of the terrorists' harmful messages in cyberspace. Hence, a need exists for a study to understand the effectiveness of cyber technologies and the choices security experts and administrators make. This study strives to advance security research by integrating findings from experts and security administrators to improve understanding of how they choose cybersecurity technologies to mitigate terrorist propaganda and networking in Nigeria cyberspace. This qualitative interview study focused on experts from five sectors (Law enforcement, Intelligence, Military, Academic, and private sector) in Nigeria. Using a qualitative interview with 15 participants, I obtained individual experts' perceptions about the

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

effectiveness and integration of cybersecurity technologies with counterterrorism strategy to stop terrorists' propaganda campaign and networking in Nigeria cyberspace. I collected empirical data on the situational factors, 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. In addition, I reviewed relevant documents such as legislation, executive orders, research papers, and transcripts of public speeches by government officials.

Assessing effectiveness and practicality of cybersecurity technologies in mitigating terrorists' networking and propaganda in Nigeria's cyberspace based on perceptions of experts enabled me to identify areas where improvements are required. 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. In this article, I highlighted the report of this study, beginning with the background, routine activity theory discussion on terrorist propaganda, cyberterrorism, and terrorist use of social media technology. The study closes with a conversation on the interpretations of findings, policy recommendations, and conclusion.

Routine Activity Theory

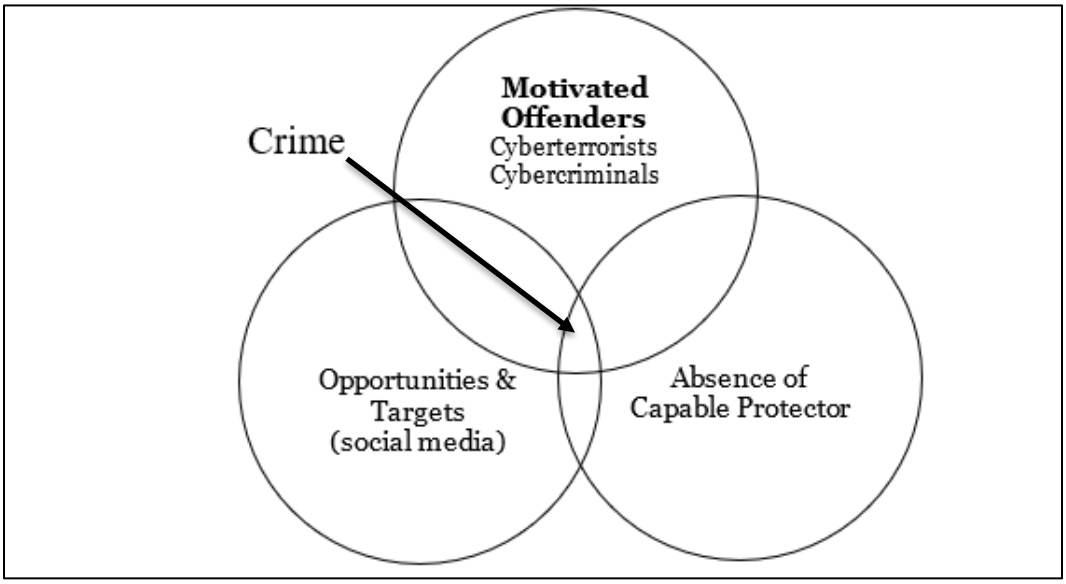
The theoretical framework for this study is Cohen & Felson's (1979) routine activity theory, which is an environmental, place-based account that three elements must be available for a crime to occur. There must be an opportunity, motivation, and vulnerable platform. The role of criminology theory such 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.[8] However, Peter Grabosky posits that the underlying

mechanism of criminality in cyberspace is the same as for real-world crimes.[9] The motivation of computer criminals is not new in the sense that they are driven by greed, lust, power, revenge, and adventure.[10] Moreover, Foley argued that routine activity is a resource that has been mostly untapped by students of counterterrorism.[11]

Routine activities of everyday life present opportunities for crime to occur. Cohen and Felson found that most criminal acts require convergence in space and time, which implies that circumstances must be right for criminal activities to take place.[12] For my study, the argument was 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.

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

Figure 1. Application of Routine Activity Theory



Source: Author.

Methodology

The study collected data holistically. The data collection includes face-to-face interviews with security experts, document content analysis of open source, non-classified 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. Qualitative research supports the "purposive" selection of key informants in the field who can assist in identifying information-rich cases.[13] With qualitative research interviews, the study focused on key players on how Nigerian government manages the terrorists networking and propaganda in cyberspace. The study 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 semi structured in-depth face-to-face interviews. In addition, I established a protocol for recording this information. Rubin and Rubin posited that the qualitative interview is appropriate when the study purports to answer "how" and "why" questions.[14] Hence, the study gathered the needed data through a qualitative interview through which it 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. 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.

Understanding Cyberterrorism

The term *cyberterrorism* is a compound of the words *cyberspace* and *terrorism*.[15] Cyberterrorism refers to a computer-aided terror act.

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

Cyberterrorism is a politically motivated attack that generates fear or harm. It should result in violence or threat of violence against persons or properties. 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 because 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.[16] 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.[17]

Robert Murril posited that the term could be misleading, and the response could be based on who is defining it.[18] "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. This set of action in cyberspace falls within the definition of cyberterrorism and will result in counterterrorism responses. Transnational terrorists use online tactics like "cyber-mobilization," and computer malware as economic weapons.[19] Terror groups around the world, including Boko Haram in Nigeria, use technology to spread violent ideology and recruit members. Early research asserted that the use of the Internet to communicate, coordinate events and actions does not necessarily constitute cyberterrorism.[20] Eliot Che 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.[21]

Nevertheless, Al Mazari et al. developed cyberterrorism taxonomies to include cyber-attacks against social and national identity.[22] 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.[23] Moreover, Martin and Weinberg 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.[24] 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 Seymour 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.[25] 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.[26]

Benson David 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,

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

and could therefore better benefit from a transnational support system buoyed by a transnational (and often anonymous) communications system.[27] 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 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.[28] Meanwhile, 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.[29] 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.[30] 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 suggests that in the same way, governments can also disseminate information in support of their interests.[31] 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 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.[32] 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.

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. In t*he Global Terror Threat and Counterterrorism Challenges Facing the Next Administration*, Hoffman Bruce argues that terrorism and media are joined together in an intrinsically symbiotic relationship, each feeding off, and utilizing the other for its purposes.[33]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.[34] In addition, Jack Moore uncovered that ISIS collaborated with other terrorist groups like Boko Haram to spread its messages and provided cyber and media training to them.[35] Through this partnership, Boko Haram was exposed to and

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

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 groups 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.

Bruce Hoffman 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.[36] Moreover, the creation of a secure environment, including comprehensive and integrated information operation (IO) are critical factors to consider for counterterrorism operations.

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.[37] In today's world, social media outlets have become part of daily life with terrorists using these media to send messages of fear. 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, using Twitter.[38] 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.[39] Social media has fueled the recent upsurge of lone wolf terrorism around the world.[40]

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.[41] 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.[42]How terrorists use social media to perpetrate its agenda points to the future. Lohrmann found that ISIS has been using the Internet successfully to recruit new fighters through new media technology such as Facebook, Twitter, YouTube, and Telegram.[43] 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 discovered that the application of social media technology such as Twitter, Facebook, Instagram, Telegram, and

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

Chatroom facilitated communication and coordination at a global level outside of the control of governments.[44] 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 are 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.[45]

In addition, a report titled "The evolution of terrorist propaganda: The Paris attack and social media" by the U.S. 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.[46] 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 consists of right resources, tools, and process to defend against cyberterrorism.[47] 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 explained that AI-based security applications can read and understand security — they can analyze every incident,

identify causes, methods, and trends, and predict the next pattern even before it happens.[48] For instance, IBM developed Watson, which has been taught to read vast quantities of information online.[49] 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 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.[50] 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 argues that the ability to operate undetected while using online tactics makes terror groups real beneficiaries of cyberspace technology.[51] Terrorist enjoys the anonymity the cyberspace provides them. Stealth is the most significant advantage of the Internet. Kaplan pointed out that terrorists swim in the ocean of bits and bytes, which make it difficult to identify the real culprits or bad actors.[52] The secure means of communication through encryption tools, steganography, dead dropping (transmitting information through saved draft emails 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

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

deception and failure in cyberspace just like the same protection that the cyber technology offers the group.[53]

In Schultz's study, it recommended false-flag operations (FFO) 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. In addition, 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 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.[54] 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.

Adomi and Igun described 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.[55] 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 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.[56] For instance, many of ISIS' foreign fighters were recruited through social media platforms.[57] 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.[58]

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

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

committed actors who are motivated by ideology, religion, or political agendas. In addition, 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 coordinates their secure conversation with the encryption technology. Fink, Pagliery, and Segall 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 now.[59]

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 proceeds of their exploits. 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	

Source: Compiled by author.

Findings and Discussion

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 do. 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.

It is known that terrorist organizations are using online tactics to spread fear, panic, and present situations of uncertainty to the public. 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. 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.

In addition, 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 we know from the literature review that

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

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 creates 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.

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. Routine Activity Theory 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.

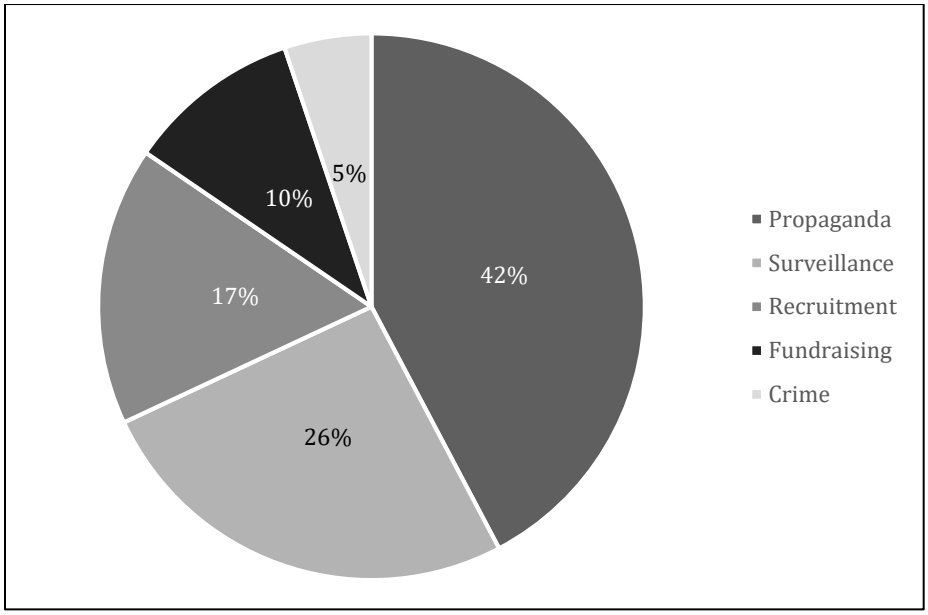
Table 2. Names Provided by Interviewees of Selected Terrorist Organizations and Separatist Movements Known to Be Active in Nigerian Cyberspace

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

Source: Compiled by author.

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

Figure 2. Cyber activities of Nigerian Terrorists Identified by Interviewees.



Source: Author.

What Experts are Saying About Cybersecurity Technologies

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 leadership to make technology effective. In addition, 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.

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."

Varieties 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. In addition, 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. 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.

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. 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

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

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. In addition, 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. In addition, 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. In addition, 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 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.[60] 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.

Experts 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. In fact, with artificial intelligence it is possible for security administrators to identify perpetrators and even block messages before they become public. In addition, the ability to trace activities back to the offenders with modern digital forensic tools is an added advantage. Meanwhile, all the participants pointed to lack of expertise within the intelligence and law enforcement agencies to apply the technologies effectively. Of course, while technology is good and effective, the authorities lack 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. A need exist for the Nigerian government to 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 indicates that the authority relies more on foreign experts and technologies.

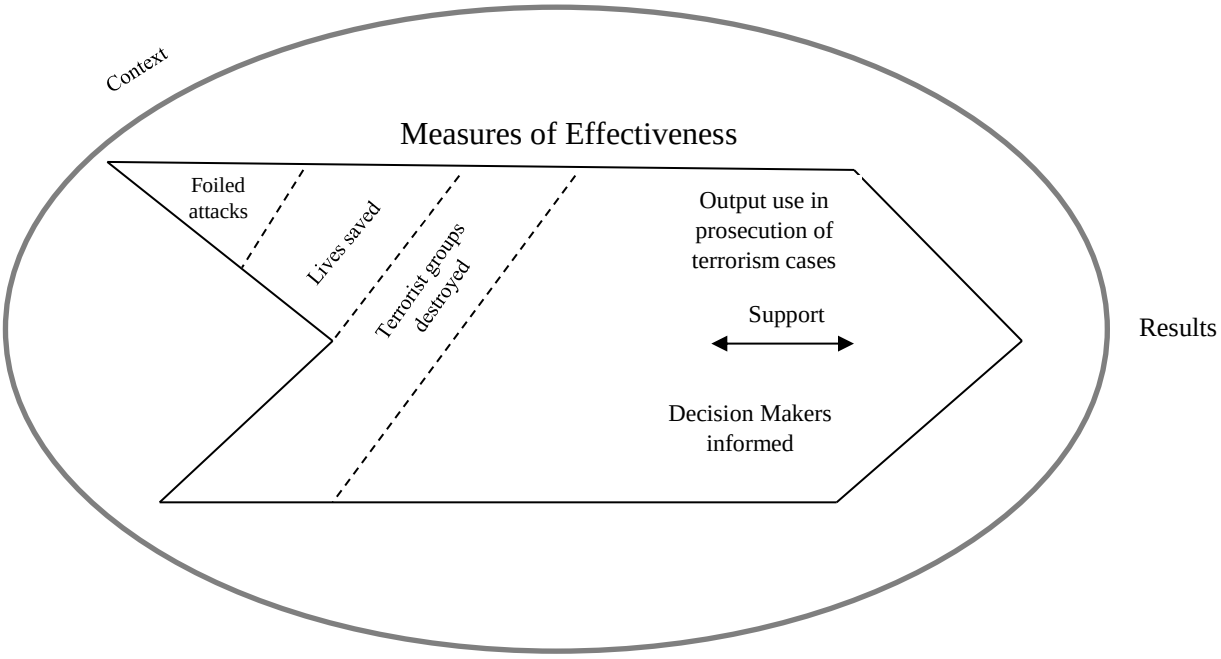
However, participants agreed that cybersecurity technologies are not a total panacea, but that the long-term strategy should be based on an educational program, deepening democratic culture, alleviating poverty, and expansion of opportunities for young people. The implication and interpretation are that technology alone cannot be used to fight terrorism and secure cyberspace. Their use must be comprehensive and

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

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 and Pieters point out that effectiveness is an impact that is desirable and recognized as contributing towards sought-after security goals.[61] In addition, 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.

Figure 3. Evaluating the Effectiveness of Cybersecurity Technologies as Described by Security Experts.



Source: Author.

Moreover, 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. In addition, 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. 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[62]. My study has confirmed that law enforcement and intelligence agencies are helpless without the full cooperation of the technology companies. In addition, the study confirms that weak leadership, nepotism, corruption, and lack of technological expertise 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

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

cyberspace. Boko Haram and 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.

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 addition, 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 above, I present some recommendations below with a focus on how to advance the efforts to mitigate the expansion and organization of terrorism in cyberspace.

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. Consideration 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

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

the last US election, nation-state actors like Russia should replicate this study with a focus on information operations.

Recommendations for the Nigerian Government

First, based on the assessment of Research Question, 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.[63]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.

In addition, 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.

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 cyber threats, including terrorists' activities in online platforms cannot be overemphasized.

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.

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

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.

Endnotes

[1] Osho Oluwafemi, Falaye Adeyinka Adesuyi, and Shafi'I M. Abdulhamid ,"Combating Terrorism with Cybersecurity: The Nigerian Perspective" *World Journal of Computer Application and Technology* 1, no. 4 (2013): 103-109, http://www.hrpub.org/journals/article_info.php?aid=909.
[2] Aliyu Odamah Musa, "Socio-economic Incentives, New Media and the Boko Haram Campaign of Violence in Northern Nigeria," Journal of African Media Studies 4, no. 1 (2012): 111-124., https://doi.org/10.1386/jams.4.1.111_1.
[3] Aliyu, "Socio-economic Incentives, New Media and the Boko Haram Campaign of Violence in Northern Nigeria."
[4] US Army Training and Doctrine Command. "*Critical Infrastructure."*
[5] Kaplan, Eben. "Terrorists and the Internet." *Council on foreign Relations* 8 (2009).
[6] Adomi, Esharenana E., and Stella E. Igun. "Combating cyber crime in Nigeria." *The Electronic Library* 26, no. 5 (2008): 716-725.
[7] Berger, John M. "The evolution of terrorist propaganda: The paris attack and social media." *The Brookings Institution* (2015).
[8] Reyns, Bradford W., Billy Henson, and Bonnie S. Fisher. "Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization." *Criminal justice and behavior* 38, no. 11 (2011): 1149-1169, doi.org/10.1177/0093854811421448.
[9] Grabosky, Peter N. "Virtual criminality: Old wine in new bottles?." *Social & Legal Studies* 10, no. 2 (2001): 243-249.
[10] Grabosky, "Virtual criminality: Old wine in new bottles?"
[11] Foley, Frank. "Reforming counterterrorism: Institutions and organizational routines in Britain and France." *Security Studies*18, no. 3 (2009): 435-478, doi:10.1080/09636410903132920
[12] Cohen, Lawrence E., and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach (1979)." In *Classics in Environmental Criminology*, pp. 203-232. CRC Press, 2016. http://www.personal.psu.edu/users/e/x/exs44/597b-Comm%26Crime/Cohen_FelsonRoutine-Activities.pdf
[13] Creswell, John W. "Qualitative Inquiry & Research Design Choosing Among Five Approaches. Sage Publications." *Thousand Oaks, CA* (2007).
[14] Rubin, Herbert J., and Irene S. Rubin. *Qualitative interviewing: The art of hearing data*. Sage, 2011.
[15] Minei, Elizabeth, and Jonathan Matusitz. "Cyberspace as a new arena for terroristic propaganda: an updated examination." *Poiesis & Praxis* 9, no. 1-2 (2012): 163-176, https://link.springer.com/article/10.1007/s10202-012-0108-3.
[16] Al Mazari, Ali, Ahmed H. Anjariny, Shakeel A. Habib, and Emmanuel Nyakwende. "Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies." In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, pp. 608-621. IGI Global, 2018.
[17] Douglas, Schweitzer. "Be prepared for cyberterrorism," *Computerworld,* March 28, 2005,https://www.computerworld.com/article/2556419/security0/be-prepared-for-cyberterrorism.html.
[18] Robert, Murrill. "The Question Of Cyber Terrorism," *Forensic Focus,* July 23, 2011, https://articles.forensicfocus.com/2011/07/23/the-question-of-cyber-terrorism/
[19] Martin, Susanne, and Leonard B. Weinberg. "Terrorism in an era of unconventional warfare." *Terrorism and political violence* 28, no. 2 (2016): 236-253.
[20] Denning, Dorothy E. "Cyberterrorism." (2000), http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

[21]. Che, Eliot. *Securing a Network Society: Cyber-terrorism, International Cooperation and Transnational Surveillance*. Research Institute for European and American Studies (RIEAS), 2007.
[22]. Al Mazari et al., "Cyber terrorism taxonomies."
[23]. Rogan, Hanna. "JIHADISM ONLINE-A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes." *FFI/Report* 915 (2006): 2006., http://aseanregionalforum.asean.org/files/Archive/16th/ARF-Conference-on-Terrorist-Use-of-the-Internet-Bali-6-8November2008/Stinson's%20Presentation/JIHADISM%20ONLINE%20AQ%20AND%20GPS.pdf
[24]. Martin et al., "Terrorism in an era of unconventional warfare."
[25]. Goodman, Seymour E. "Cyberterrorism and Security Measures." *Kumar, Arvind et al, eds* (2007): 43-54.
[26]. Conway, Maura. "Reality bytes: cyberterrorism and terrorist'use'of the Internet." *First Monday* 7, no. 11 (2002). 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
[27]. Benson, David C. "Why the internet is not increasing terrorism." *Security Studies* 23, no. 2 (2014): 293-328.
[28]. Minei, Elizabeth, and Jonathan Matusitz. "Cyberspace as a new arena for terroristic propaganda"
[29]. Weimann, Gabriel. "Virtual disputes: The use of the Internet for terrorist debates." *Studies in conflict & terrorism* 29, no. 7 (2006): 623-639. doi.org/10.1080/10576100600912258
[30]. Jack, Moore. "ISIS supporters call for poisoning..."
[31]. Benson, "Why the internet is not increasing terrorism."
[32]. Benson, "Why the internet is not increasing terrorism."
[33]. Hoffman, Bruce. "The Global Terror Threat and Counterterrorism Challenges Facing the Next Administration." *CTC Sentinel* 9, no. 11 (2016): 1-8.
[34]. McDowell-Smith, Allison, Anne Speckhard, and Ahmet S. Yayla. "Beating ISIS in the digital space: Focus testing ISIS defector counter-narrative videos with American college students." *Journal for Deradicalization* 10 (2017): 50-76.
[35]. Jack, Moore. "ISIS supporters call for poisoning of food in grocery stores across U.S. and Europe," *Newsweek,* September 7, 2017, https://www.newsweek.com/isis-supporters-call-poisoning-grocery-stores-us-and-europe-660750?utm_campaign=NewsweekFacebookSF&utm_source=Facebook&utm_medium=Social
[36]. Hoffman, Bruce. "The Coming ISIS–al Qaeda Merger." *Foreign Affairs* (2016), https://www.foreignaffairs.com/articles/2016-03-29/coming-isis-al-qaeda-merger
[37]. Rogan, Hanna. "JIHADISM ONLINE-A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes." *FFI/Report* 915 (2006): 2006., http://aseanregionalforum.asean.org/files/Archive/16th/ARF-Conference-on-Terrorist-Use-of-the-Internet-Bali-6-8November2008/Stinson's%20Presentation/JIHADISM%20ONLINE%20AQ%20AND%20GPS.pdf
[38] Berger, John M. "The evolution of terrorist propaganda: The paris attack and social media." *The Brookings Institution* (2015).
[39] "Encrypted app allows extremists to plot attacks without detection," *Homeland Security News Wire,* August 22, 2017, http://www.homelandsecuritynewswire.com/dr20170809-encrypted-app-allows-extremists-to-plot-attacks-without-detection

[40] Aly, Anne, Stuart Macdonald, Lee Jarvis, and Thomas M. Chen. "Introduction to the special issue: Terrorist online propaganda and radicalization." *Studies in Conflict & Terrorism*, 40(1), 1–9. doi:10.1080/1057610X.2016.1157402 (2017): 1-9.
[41] Baken, D. "Cyber warfare and Nigeria's vulnerability'." *E-International Relations* 3 (2013).
[42] Agbiboa, Daniel, and Benjamin Maiangwa. "Why Boko Haram kidnaps women and young girls in north-eastern Nigeria." *conflict trends* 2014, no. 3 (2014): 51-56.
[43] Dan, Lohmann. "How terrorists' use of social media points to the future," *GOVTECH,* June 20, 2016, http://www.govtech.com/em/safety/Terrorists-And-Social-Media.html
[44]. Liang, Christina Schori. "Cyber Jihad: Understanding and Countering Islamic State Propaganda." *GSCP Policy Paper* 2 (2015): 4., https://www.jugendundmedien.ch/fileadmin/user_upload/3_Medienkompetenz/Gegennarrative/Cyber_Jihad_-_Understanding_and_Countering_Islamic_State_Propaganda.pdf
[45]. Hubler, David. IAFIE conference concludes with calls for more intelligence education programs. *IN Homeland Security,* May 26, 2017, http://inhomelandsecurity.com/iafie-conference-concludes-calls-intelligence-education-programs/
[46]. Berger, "The evolution of terrorist propaganda."
[47]. Berger, "The evolution of terrorist propaganda."
[48]. Maria Korolov. "How AI can help you stay ahead of cybersecurity threats," *CSO Online,* October 19, 2017, https://www.csoonline.com/article/3233951/machine-learning/how-ai-can-help-you-stay-ahead-of-cybersecurity-threats.html.
[49]. Newton Lee. "Artificial Intelligence and data mining,". *Counterterrorism and Cybersecurity* (pp. 323–341). Cham.: Springer, 2015.
[50]. Mike Isaac. "Facebook and Other Tech Companies Seek to Curb Flow of Terrorist Content," *New York Times*, December 5, 2016, https://www.nytimes.com/2016/12/05/technology/facebook-and-other-tech-companies-seek-to-curb-flow-of-terrorist-content.html
[51]. Schultz, Robert William. "Countering Extremist Groups in Cyberspace." *Joint Forces Quarterly* 79, no. 4, 2015. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_54-56_Schultz.pdf
[52]. Kaplan, Eben. "Terrorists and the Internet." *Council on foreign Relations* 8 (2009).
[53]. Schultz, "Countering Extremist Groups in Cyberspace."
[54]. Thomas Holt. "Here's how terrorist groups use technology to recruit new members," *Business Insider*, April 28, 2016, http://www.businessinsider.com/heres-how-terrorist-groups-use-technology-to-recruit-new-members-2016-4
[55]. Adomi, Esharenana E., and Stella E. Igun. "Combating cyber crime in Nigeria." *The Electronic Library* 26, no. 5 (2008): 716-725.
[56]. Sageman, Marc. "Understanding terror networks." *International journal of emergency mental health* 7, no. 1 (2005): 5-8.
[57]. Foley, Frank. "Reforming counterterrorism: Institutions and organizational routines in Britain and France." *Security Studies*18, no. 3 (2009): 435-478, doi:10.1080/09636410903132920
[58]. Osho, Oluwafemi, and Agada D. Onoja. "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis." *International Journal of Cyber Criminology* 9, no. 1 (2015).
[59]. Jose Pagliery, Jamie Crawford and Ashley. "CENTCOM Twitter account hacked, suspended," *CNN,* January 12, 2015, http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/index.html
[60]. Goodman, Seymour E. "Cyberterrorism and Security Measures." *Kumar, Arvind et al, eds* (2007): 43-54.

https://scholarcommons.usf.edu/jss/vol12/iss1/4
DOI: https://doi.org/10.5038/1944-0472.12.1.1707

[61]. Cayford, Michelle, and Wolter Pieters. "The effectiveness of surveillance technology: What intelligence officials are saying." *The Information Society* 34, no. 2 (2018): 88-103. https://doi-org.ezp.waldenulibrary.org/10.1080/01972243.2017.1414721
[62]. "Countering violent extremism: Zurich-London recommendations on preventing and countering violent extremism and terrorism online," *Global Counterterrorism Forum,* September 15, 2015, https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/A/GCTF%20-%20Zurich-London%20Recommendations%20ENG.pdf?ver=2017-09-15-210859-467.
[63]. US Department of State, "Country Report 2016."