Countering Online Radicalization: Strategies for Mitigating the Threat of Lone Wolf Terrorism in Nigeria

Nweke, Chibuzor Chigozie
Department of Political Science, faculty of social sciences,
Nnamdi Azikiwe University
Awka, Anambra State

Okafor , Frank-Collins N.
Department of Political Science, faculty of social sciences,
Nnamdi Azikiwe University
Awka, Anambra State

Emelife, Anthony Maduka
Department of Political Science, faculty of social sciences,
Nnamdi Azikiwe University
Awka, Anambra State

Abstract

This study examine strategies for countering online radicalisation of lone wolf terrorist. The study was guided by three research questions. A qualitative historical research design was used in the study. The population comprises of 41,740 text documents published as open sources within the period of 2005 to 2021. The sample size for this study comprised of 96 text documents and 15 Key Informant Interviewees. A multistage sampling was used to select 96 text documents, while purposive sampling was used to select 15 Key Informant Interviewees. Data collected were analysed using thematic analysis. Results shows that terrorist groups used social media sites in disseminating propaganda on the Internet due to its in-built interactive features and popularity among people especially the youths. Through online platforms like Facebook, YouTube, Twitter, potential lone wolves were able to easily connect and identify with like-minded peers on the Internet. Further findings from the study show that monitoring and removing extremist from chat room; creation of websites to lure extremist; intercepting & hacking social media accounts; and the use of computer algorithms to identify extremist on the internet were some of the effective strategies of countering online radicalization of lone wolf. The study recommend among others that Since the Nigerian law enforcement agencies should use electronic surveillance techniques to monitor online activity and identify potential lone wolves.

Key words: *Radicalisation, Lone wolf terrorist, online radicalisation, social media, Internet, terrorism, counter-terrorism*

Introduction

Since the dawn of history, terrorism has continuously posed a critical security challenge to humanity. It has plagued mankind for, at least, the past two millennia. Right from its outset, it has attracted and continues to be a topic of discussion among scholars. Depending on how it is defined or perceived, it connotes death and mayhem. Terrorism has taken on a different dimension even as the world becomes more globalised. In recent times, there have arisen dimensions of terrorism whose style and mode of operation have made it more puzzling and unpredictable for the police and security intelligence agencies to tackle. A typical form of such terrorism is attributed to lone wolf terrorism. Unlike traditional terrorist groups, lone wolves operate independently, making them particularly difficult to detect and thwart for law enforcement and intelligence agencies.

It is not a coincidence that the internet era, which gave rise to all manner of social media platforms, also saw the rise of lone wolf terrorism. Social media are both ubiquitous and participatory (Asemah, 2011). The term is connected to a wide range of possibilities. For instance, social media offers the possibility of on-demand access to content whenever and wherever you are, on any digital device, as well as interactive user response, creative involvement, and the development of communities around the media content. The digitisation of content into bits distinguishes new media from traditional media.

Concerning the lone wolves, it has been debated that information dissemination through the various new media platforms may significantly contribute to their radicalisation. When exposed to such radical contents for a period of time, their extremist beliefs become hardened, and because the Internet provides them with anonymity and a network of peers that share their extremist beliefs, they will tend to have some sense of moral justification for using violence as a means to an end. Pantucci (2011) outright claimed that lone wolves are individuals that practically are radicalised through the internet before they engage in violent activities. For instance, the recent spate of Lone Wolf terrorism attacks in western society suggests that potential lone wolves shifted to radical actions after subscribing to radical opinions and ideologies, which were possible due to the rapid increase of radicalising information on the internet. The radicalisation information includes information on the instructions for bomb making, instructions for gaining weapons of mass destruction, or terrorist tactic guidelines. Based on Benson's (2014) assertion, criminal information of this kind actually enables lone wolves to prepare terrorist attacks and act truly independently.

Although efforts have been made to counter their activities in western countries, specifically France, Canada, the United Kingdom, Germany, and Australia. They introduced new laws surrounding technological surveillance. By virtue of these laws, these countries were able to express their counter-terrorism moves by intercepting financial transactions and online message services, such as hacking a social media account used to recruit jihadists, tapping phones, and sending emails. Others include the use of force on internet providers to install complex algorithms that will identify online suspect behavioural patterns using keywords, sites visited, and contacts made, and also have the power to monitor by accessing a limitless number of computers (ABC, 2015; Chrisafis, 2015; Grubb, 2014).

Despite these efforts put in place, lone wolf terrorism in the United States of America and notable European nations is on the rise (Hennigan, 2018; Wray, 2020). The reason being that a greater number of vulnerable Americans, Europeans, and even Africans that tend to be susceptible and sympathetic to violent messages are still being spotted, accessed, and radicalised online.

The radicalisation of people and their recruitment for violent and illegal activities through online platforms is no longer a new phenomenon in Africa (Sirkku, 2016). In his investigation into the patterns of terrorist activity in relation to internet availability across the Sahel countries of Africa, Coulombre (2021) found a direct correlation between the frequency of terrorist attacks that have occurred in Chad, Mali, Niger, and Sudan since the year 2000 and the countries' increased internet accessibility. In sub-Saharan Africa, terrorist organisation has leverage on the Internet to promote its propaganda (including in French and English) through more sophisticated films. "Boko Haram" for instance have deviated from regional norms of communication by posting propaganda videos to agencies on flash drives or CD-ROMs and by being present on the most popular social media platforms (Twitter, Instagram) (Olivier, 2015). Moreover, the group multiplies its activities on Twitter, especially via their smartphones, as well as through YouTube news channels. Most tweets and comments from the group's supporters denounce the Nigerian government and call for support for the "Boko Haram" movement.

Clearly, it can be deduced that the dimension of radicalisation of a person or persons into a terrorists via the Internet poses a serious threat to Nigeria. Supporting this view, Apau (2020) opined that as vulnerable developing nations are gaining more access to the internet, terrorists would probably try to capitalise on the newfound access to these hard-to-reach audiences around the world. In fact, the state of insecurity and the lack of capacity to counter it makes her more vulnerable to online radicalisation of lone wolf terrorists. On this note, the study sets out to investigate strategies for countering online radicalisation of lone wolf terrorist.

Research questions

From the above discussion, the following research questions emerged:

1. How do extremist groups exploit the internet for terrorism purposes?
2. How does the internet enable the radicalisation of lone wolf terrorist?
3. What strategies are deploy in countering the radicalisation of lone wolf terrorist?

1.2 Purpose of the study

The main purpose of this paper is to examine strategies for countering online radicalisation of lone wolf terrorist. The specific objectives are:

1. examine how extremist groups exploit the internet for terrorism purposes;
2. Analyze how the internet enable the radicalisation of lone wolf terrorist; and
3. examine approaches adopted by other nations to address lone wolf threats.

The paper is divided as follows: Section 2 offers a scholarly examination of the literature pertaining to how extremist groups exploit the internet for terrorism purposes, how the internet enables radicalisation of lone wolves and strategies that are used for counteracting radicalization of lone wolves terrorist. Section 3 presents the theory upon which the paper was anchored. Section 4 is on the methodology deployed. Section 5 highlights the results and findings of the paper. Section 6 concludes the paper. Finally, section 7 provides recommendation.

2.0 Literature review

2.1 How extremist groups exploit the internet

The Internet and new media platforms have emerged as significant tools for extremist groups, providing multifaceted avenues for various activities such as research, propaganda dissemination, communication, training, recruitment, and coordination of attacks (Theohary & Rollins, 2011; Thompson, 2011; UNODC, 2012; Weimann, 2005, 2010, 2011). These capabilities stem from the Internet's efficiency in information gathering and sharing, facilitating tasks ranging from identifying target locations through platforms like Google Maps to distributing bomb-making manuals (Woodring, 2014). Recent studies highlight the rapid adoption of new social media platforms by extremist groups to advance their agendas, recruit members, and radicalize individuals (Brachman, 2006; Freiburger & Crane, 2008; Jenkins, 2010, 2011; Theohary & Rollins, 2011; Thompson, 2011; UNODC, 2012; Weimann, 2005, 2010, 2011).

The Internet's expansion has introduced a plethora of tools for terrorist utilization. Besides practical applications, new social media facilitates the promotion of extremist ideologies, which are often as much about identity expression as they are about belief systems, particularly evident in homegrown violent extremists (Meehan et al., 2011). Social networking sites (SNSs) have become pivotal, with 90% of terrorist activities online occurring within these platforms (Weimann, 2010). The proliferation of jihadist websites and chat rooms, coupled with the rise of English-language platforms, has widened the accessibility of radical narratives (Jenkins, 2010). Major SNSs like Facebook, Twitter, and YouTube offer real-time updates and global reach, presenting both opportunities for expansion and threats of amplifying extremism (Klausen et al., 2012).

Facebook, with its vast user base, poses significant security challenges, as terrorists exploit it for friendship establishment and targeted messaging (Weimann, 2010). Similarly, Twitter enables real-time logistics updates, potentially aiding in military ambushes (Weimann, 2011). The Internet's role in radicalization extends beyond practical utility, encompassing psychological impacts, with propaganda disseminated swiftly to influence vulnerable individuals (Brachman, 2006; Freiburger & Crane, 2008; Jenkins, 2011; Silber & Bhatt, 2007).

Concerning lone wolves, the internet serves as a vital repository of information on tactics and weaponry, facilitating independent terrorist acts (Benson, 2014). Although face-to-face communication remains paramount in attack planning, online resources provide essential knowledge and ideological reinforcement (Mueller & Stewart, 2015). Terrorist organization websites primarily focus on self-propagation rather than practical instruction, using rhetoric to justify violence and indirectly influence visitors towards radicalization (Brandon, 2008; Tsfati & Weimann, 2002)

2.2Radicalization of lone wolf terrorist and the internet

Radicalization is a complex process by which individuals or groups come to embrace increasingly extreme views that challenge the status quo (McCauley & Moskalenko, 2008). This could be challenging existing social, political, or religious order. This shift is not simply adopting a dissenting opinion; it is a movement towards violence as a means for change. Scholars still grapple with a precise definition of "extremist views" and the line between acceptable protest and radicalization (Alfaro-Gonzalez et al., 2015). However, Hafez and Mullins (2015) offer a helpful perspective, defining radicalization as a gradual process of adopting an extremist ideology that justifies violence as a legitimate tool for social or political change. It is important to note that radicalization does not guarantee violence, but it sets the stage for it.

While a universally agreed-upon definition remains elusive, there is consensus that radicalization is a process influenced by various factors (Alfaro-Gonzalez et al., 2015). Hafez and Mullins (2015) categorize these factors as ideological, psychological, social, political, economic, and technological. Individuals who feel isolated or disconnected from their communities may be more susceptible to extremist narratives that offer a sense of belonging and purpose. Feelings of marginalization, discrimination, or political disenfranchisement can create fertile ground for extremist ideologies that promise change and empowerment. Propaganda and messaging from extremist groups can be persuasive, especially for individuals already experiencing vulnerability (Bergsen & Bjørgo, 2015). Social media platforms can be particularly effective tools for disseminating extremist content (Marcks & Pawelz, 2020).

Technology is increasingly seen as a significant factor contributing to radicalisation. For example, Islamic States have been incredibly successful in recruiting young fighters from around the world by posting slick propaganda videos on YouTube, Twitter, Facebook and other social media platforms (Greenberg, 2016; Klausen, 2015; McDowell-Smith, Speckhard, & Yayla, 2017). As Greenberg (2016) explains, this approach speaks directly to the youth, as it is targeted to them for the purpose of recruitment, using the medium that works best for the youth. To buttress the significant role of technology to radicalisation, Alfaro-Gonzalez et al. (2015) mentioned that Islamic State's world reach would not have been possible without the Internet.

In the radicalisation of lone wolf terrorists, the internet also play a significant role in the path towards lone wolf terrorism. Studies suggest that online exposure played a role in the decision to commit an act of terror. Gill et al. (2017) found that 14% of lone wolf terrorists in the UK studied (between 1990 and 2014) decided on violence after online exposure. Some of the phases that leads to facilitates radicalisation and subsequently terror by lone wolf terrorist are summarised below (Guri & Ravndal, 2021):

Pre-existing vulnerabilities

Vulnerable individuals may seek alternative worldviews online due to dissatisfaction with existing social, political, or economic systems (Guri & Ravndal, 2021). This exposure can make them more receptive to extremist narratives. However, researchers rarely conclude that online content alone causes radicalisation (Borum, 2011). Pre-existing vulnerabilities, often called "push" and "pull" factors, play a significant role (Borum, 2011; Neo, 2016). "Push" factors are pre-existing grievances that make individuals susceptible to extremist narratives. "Pull" factors are the specific ideologies encountered online that resonate with those vulnerabilities. These vulnerabilities can make individuals more open to challenging their existing beliefs, potentially leading them down a path of radicalisation.

Isolation

Social isolation plays a significant role in subscribing into extremist views. Individuals feeling alienated offline may seek belonging online in extremist communities. This "online immersion" can deepen as real-life connections weaken (Bergin et al., 2009). Sageman (2008) emphasizes the importance of virtual communities for lone actors who find a sense of belonging online. Online forums can become a place to connect with those who share their views, even if those views are not widely held in their offline communities. This online immersion can coexist with offline isolation, creating a cycle that reinforces radicalization (Bergin et al., 2009; Sageman, 2008). Isolation can occur at various stages. It can start with alienation from society, making someone more receptive to radical narratives (Weimann & Von Knop, 2008). Later, it can manifest as withdrawal from real-life relationships due to the online community taking precedence (Malthaner & Lindekilde, 2017; Torok, 2013).

The role of online facilitation

The online environment can promote exposure to extremist content (von Behr et al., 2013). The internet acts as a facilitator by providing a platform for information, communication, and propaganda (von Behr et al., 2013; Gill et al., 2017). This facilitation can streamline the radicalisation process by offering both ideological development and resources for planning attacks (Weimann & Von Knop, 2008). Online environments can facilitate both the radicalization phase (ideological development) and the operational phase (planning attacks).

2.3 Successful approaches adopted by other nations in addressing lone wolf threats

Preventing terrorist attacks remains a paramount objective for the American government, particularly in the context of the emergence of Lone Wolf terrorism. Countering the actions of Lone Wolf terrorists poses significant challenges, yet there are measures to mitigate their activities. These include efforts to counter radicalization, combat terrorism financing, and conduct surveillance of Lone Wolves online.

Radicalization, a precursor to terrorist acts, occurs not only through online channels but also within prisons and communities, both domestically and internationally. In response, various programs have been implemented to address the threat of radicalization and homegrown terrorism in the United States. For instance, the Obama administration established a counter-radicalization strategy in 2011, with a focus on individuals potentially inspired by Al Qaeda (Wray, 2020). Subsequently, the Trump administration restructured the Office for Community Partnerships into the Office of Terrorism Prevention Partnerships, emphasizing education and community awareness to identify signs of radicalization and suspicious behavior (Wray, 2020).

Since the September 11 attacks, tracking and disrupting terrorist financing have been key components of US counter-terrorism efforts. The Patriot Act expanded the Treasury's authority to detect and prosecute individuals suspected of money laundering and terrorist financing . The United States also plays a leading role in the Financial Action Task Force on Money

Laundering, which addresses terrorist financing by developing policies and recommendations for member countries (Wray, 2020).

Furthermore, surveillance of Lone Wolves on the internet is crucial for countering terrorist activities. While the extent of internet use by Lone Wolves remains debated, it is widely acknowledged that they frequently utilize online platforms for various purposes, including expressing their ideologies and engaging in discussions with like-minded individuals. Identifying potential Lone Wolf terrorists online necessitates the use of automatic or semi-automatic search tools, as the vastness of the internet precludes manual monitoring. Semi-automatic search engines, capable of analyzing online behaviors and identifying warning signs, are deemed effective in this regard (Cohen et al., 2014).

Key warning behaviors exhibited by potential Lone Wolves include leakage, fixation, and identification. Leakage involves communicating intent to harm to a third party, often accompanied by direct threats, while fixation entails an intense preoccupation with a target, leading to extensive information gathering. Identification manifests as a desire to emulate previous attackers or align oneself with their ideologies (Meloy & O'Toole, 2011; Cohen et al., 2014).

Despite the potential of semi-automatic search tools, challenges remain in their implementation. These include translation services for multilingual content, sentiment analysis to identify problematic users or websites, mapping websites for text analysis, and author recognition to identify users based on their writing style . While algorithms are being developed to enhance language-based identification, practical limitations persist in large-scale implementation (Cohen et al., 2014).

Recent studies have analyzed online forums to better understand the behaviors and patterns of potential Lone Wolves (Scrivens et al., 2018). However, further research and technological advancements are needed to improve the efficacy of online surveillance and identification of Lone Wolf terrorists.

3.0 Theoretical framework

Social identity theory, developed by Henri Tajfel and John Turner, proposes that a significant portion of an individual's self-concept stems from their perceived membership in social groups (Tajfel & Turner, 1979). The foundation of the theory lies in the work of Henri Tajfel, who explored the concept of social identity in the 1970s (Tajfel, 1974). John Turner further refined the theory, emphasizing the interplay between personal and social identities (Turner et al., 1987). Their research demonstrated that individuals strive to maintain a positive social identity, often by associating with groups perceived as superior and denigrating out-groups (Tajfel & Turner, 1979).

Social identity theory suggests that online extremist groups exploit this need for positive social identity. These groups cultivate a sense of in-group belonging and purpose, often through shared narratives of grievance, victimhood, or a fight against a common enemy (Berghuijs & Hopkins, 2019). By portraying themselves as a cohesive and morally righteous group, they offer individuals a sense of identity and belonging that may be lacking in their offline lives (Martin et al., 2017).

Online anonymity can further exacerbate this effect. Detachment from real-world consequences can embolden individuals to explore extremist ideologies and engage with radical content they might otherwise avoid (Van der Linden et al., 2020). The echo chambers created by social media algorithms can further reinforce these in-group narratives, limiting exposure to counter-narratives and fostering a sense of groupthink (Bakker et al., 2018).

Social Identity Theory sheds light on the psychological factors that make individuals susceptible to online radicalization, particularly the allure of belonging and purpose offered by extremist groups. Understanding these motivations is crucial for developing effective counter-radicalization strategies (Gebhard et al., 2019).

By focusing on fostering positive and inclusive online communities that address underlying needs for belonging and purpose, it may be possible to provide individuals with alternatives to extremist narratives. Additionally, promoting critical thinking skills and media literacy can equip individuals to navigate online content more discerningly and challenge extremist narratives (Maréchal et al., 2019). This theory offers valuable insights into how online spaces can be breeding grounds for radicalization, particularly for individuals seeking a sense of belonging and purpose.

Social identity theory, while insightful, has limitations. It primarily focuses on in-group/out-group dynamics and may not fully capture the complexities of individual motivations for joining extremist groups (Byford, 2017). Factors like personal experiences, psychological vulnerabilities, and exposure to charismatic leaders can also play a significant role (Kalyuzhnova et al., 2018). Critics argue that the theory oversimplifies the process of radicalization and may not adequately account for ideological convictions that transcend group affiliation (McCauley & Moskos, 2008).

Furthermore, the theory focuses on the individual's perspective and doesn't fully address the role of online platforms in promoting radicalization (Alim et al., 2018). Social media algorithms that prioritize engagement can create echo chambers and exacerbate the spread of extremist content (Bakker et al., 2018). Addressing these broader societal factors is also crucial for effectively countering online radicalization. Nevertheless, the theory provides valuable insights into the psychological appeal of online extremism. By understanding the need for belonging and the allure of a shared identity within extremist groups, security agencies can develop more effective strategies to counter online radicalization efforts and mitigate the threat of lone-wolf terrorism in Nigeria.

4.0 Methodology

The study adopted a qualitative historical research design. This research design was used in this study because, it enabled the researcher examine the security measure put in place by the government of the United States of America and notable European nations in countering the radicalisation of lone wolf terrorist. Data obtained from the past events was used to examine the Nigerian state for increased susceptibility to lone wolf terrorism. The purpose of historical research according to Špiláčková (2012) is to verify and explain the history of any area of human activities, subjects or events by means of scientific processes. Importantly, historical research enables one to search and identify the relationship of past happenings and their links with the present (Berg, 2012). The design is considered appropriate for this study because secondary data on the association between lone-wolf terrorism and socioeconomic disparity were analyzed. The credibility and validity of research findings drawn from the secondary data was also boost up by primary data. 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.

5.0 Results

5.1 How extremist groups exploit the internet

The result of this study revealed that social media sites were used the most for disseminating propaganda on the Internet. The Internet through various social media platforms have made the dissemination of all manner of extremist content easy nowadays. Data from interviewees, emphasized the contemporary digital landscape, highlighting the ease with which information can be accessed and disseminated online. They expressed concern regarding the limited restrictions imposed by many social media platforms on the content traversing their networks. Drawing on their experience, they identified YouTube, Twitter, and websites affiliated with terrorist organizations as the primary vectors for extremist propaganda dissemination. One of the respondent interviewed stated that: "*There is no doubt that we are living in an era of digitisation that has made access and dissemination of information as easy as blinking the eyes. Unfortunately, most social media sites have almost zero restrictions on the type and nature of information that is propagated through their platforms. From our experience, we have come to the conclusion that YouTube, Twitter, and websites created by terrorist organisations are used most often to propagate propaganda*." Among the social media sites, exploited by extremist groups were Facebook, Internet chat rooms, YouTube, Twitter, Internet sites, and E-mail. Supporting this finding, a great number of the respondents interviewed stated that: "*Social media sites have turned into a very potent weapon in the hands of some criminal elements to carry out all forms of terrorist activities ranging from recruitment, radicalization, and training.*" In summary, social media platforms are adopted for terrorist activities due to their built-in interactive features and their wide popularity among people, especially youths. This finding is supported by the report of Wagenaar (2010), who reported that social media sites and websites harbour individual extremists and can be used as a platform for extremist organisations. For instance, social media platforms such as Facebook, YouTube, and Twitter are known to be popular among people. This is because they form complete, functioning communities aimed at the exposition of social networks (Boyd, 2008). Through the creation of a profile on a social media site, it is possible to highlight the most important aspects of one's identity for friends and peers to view, interpret, and judge. For this reason, extremist groups use mainstream media, such as YouTube and Facebook, and general religious or political websites because they know these sites can attract youth (Arts & Butter, 2009; Weimann, 2010). Social media platforms have made it easy and cheap to upload and watch information and videos from any part of the world. Because of this, access to extremist material is strongly increased, and a much broader audience is reached (Conway, 2012).

5.2 How internet enables the radicalisation of lone wolf terrorist

According to summary reviews on the roles internet played in aiding self-radicalisation of lone wolf, five themes emerged which are: firstly, the internet facilitates the connection and identification of like-minded peers; secondly, it provides anonymity for potential lone wolves; thirdly, it enables participation and engagement in terrorism discourses; fourthly, it exposes potential lone wolves to radical or extremist content; and lastly, it serves as a locus for convenient access to radicalising materials, including training manuals and videos. Through new media platforms like Facebook, Youtube, Twitter and Internet sites, lone wolves were able to engage in self-radicalisation by connecting and identifying like-minded peers on the Internet. Every forms of obstacles like geography and space in connecting individuals are reduced by the reach and immediacy of the internet. Several studies demonstrate how the internet can "reach" people who would not otherwise be accessible to radicalizers in any other way (Neumann, 2011). These studies suggested that the internet has broken down some of the barriers that exist in the physical world for certain groups of people to become involved in extremism. It has allowed easy and convenient means of conversation between disconnected and scattered people, which was not possible before.

Further findings from the study show that the Internet facilitated the self-radicalization of Lone Wolves by providing anonymity for potential Lone Wolves on the Internet, allowing for the participation and engagement of people who are already vulnerable to terrorism discourses. In line with this finding, the majority of the personnel interviewed stated that "*Social media sites offer vulnerable persons easy and constant access to information that can enable self-radicalization. By vulnerable persons, I mean persons that can easily subscribe to ideas or beliefs that are against the generally accepted laws of the land. The information they get on the Internet feeds the newly established radical view, which makes them more radicalised. The new feeling will then push them to seek out more and more radical information on the internet. Since all of their activities on the Internet can be carried out anonymously, they may further their course by searching for others who share similar radical views as theirs. At this point, they isolate themselves from normal social life and begin to live most of their lives on the Internet*". Relating these findings with results obtained in the literature, Schmidle (2009) reported that radicalization was possible via the Internet because the internet affords greater anonymity to potential Lone Wolves. It was also reported that, through the Internet, the mass of participants voicing their opinions and taking part in the theoretical reflection and advancement of the ideology directly contributes to updating the ideology and making it more attractive for potential Lone Wolves (Koehler 2014). Confidence building and affirmation also stand out in some of these more radical statements as another opportunity provided by the Internet, which supports individuals through building a perception of anonymity. The Internet provides an opportunity or fulfils an opportunity to present potential Lone Wolves as being more than they actually are. The Internet provides the major basis for ideological development and advancement through the potentially unlimited number of individuals participating, for instance, in theoretical discussions. Some academics hypothesised that because of comparable, self-imposed restrictions, introverted people may benefit from having easier access to radicalisation online (Torok, 2010; Transnational Terrorism, Security, and the Rule of Law, 2008; Yeap & Park, 2010).

The results of this study show that social media sites and Internet sites aid the self-radicalization of Lone Wolves terrorists by exposing potential Lone Wolves to radical or extremist contents that are indoctrinating and also providing them with a locus for easy access to radicalising materials, training manuals, and videos that will enable them to carry out violent acts. This result is similar to the finding of Koehler (2014), who found that the Internet provides a space for terrorists and extremists to share uncensored information connected to their chosen lifestyle, such as banned literature, images, videos, and manuals. Some of the extremist contents could be instructions on how to use local materials to make explosives, how and where to source materials that can be used for mass destruction, and directives on how and where to launch attacks.

5.3 Strategies deployed in Countering the Radicalization of Lone Wolf Terrorist

Under this section, data on how lone wolf terrorism was counteracted, as shown in past studies are revealed. From the analysis carried out, two broad themes and six sub-themes emerged as strategies for countering the activities of lone wolf terrorist. The themes are high-lighted in Figure 1 as shown below.

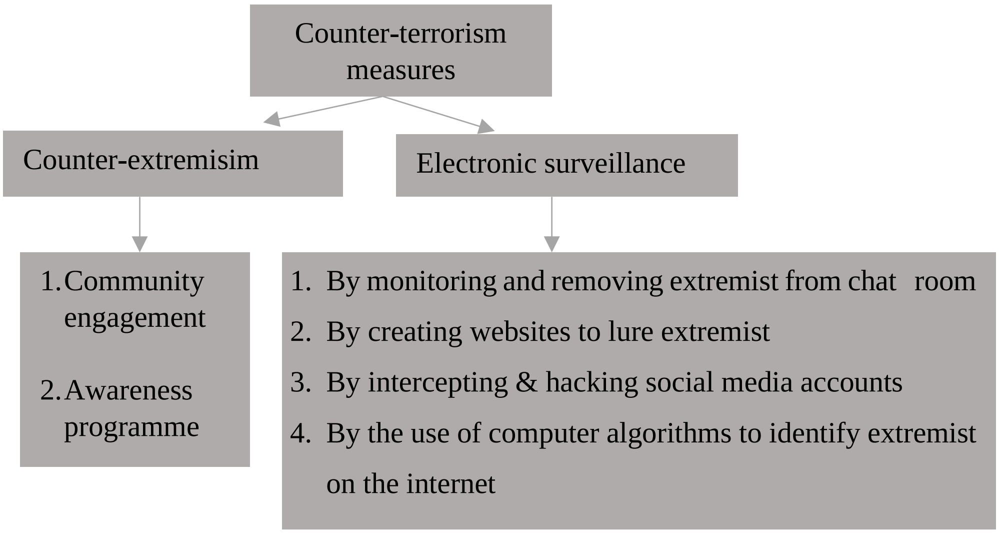
Counter-terrorism measures
Counter-extremisim
Electronic surveillance
1. Community engagement
2. Awareness programme
1. By monitoring and removing extremist from chat room
2. By creating websites to lure extremist
3. By intercepting & hacking social media accounts
4. By the use of computer algorithms to identify extremist on the internet

Fig 1: Strategies for countering lone wolf terrorism

Data in Fig 1 revealed that, lone wolves terrorism were countered in the United States of America and Europe, by putting in place, structures in localities that are prone to extremist ideologies, to de-radicalise persons that may have been immersed in radicalisation and also to prevent and protect persons from falling prey in the web of radicalisation. The structures put in place, counteracted the activities of lone wolves terrorism by way of educating, enlightening and discouraging people on the use of terrorism as a means to an end. Aside creating awareness on the negative consequences of the use of terrorism to achieve a goal, community members such religious leaders, elder statesmen etc., were also engaged to preempt radicalisation and ensure effective cooperation between community members and the security agencies. This way, communities felt supported by their government, by this move, people came forward to report behaviours that is of concern to their community leaders.

Instead of approaching the problem of lone wolf terrorism from a counter-extremisim perspective, the electronic surveillance mechanisms were also deployed in countering the activities of lone wolves terrorist (Fig 1). Data in Fig 1 shows that electronic surveillance in the form of monitoring and removing extremist from chatrooms was used as a way to combat activities that may lead to terrorism. The creation of websites to lure extremist, intercepting and hacking social media accounts of suspected extremist, and the use of computer algorithms to identify extremist activities on the internet were the other electronic surveillance measures used in combating the activities of lone wolves terrorism as revealed in literature.

It is no news that Nigeria has been tackling terrorism for over a decade now including terrorist propaganda online. However, Nigeria has made little progress in countering terrorist propaganda on the Nigerian cyberspace. Reasons been that the country lack expertise that possesses the requisite technical skills to dismantle terrorists' websites and counter their messaging on social media platforms and due to the ineffective government's counter narrative efforts on social media. This finding is similar to that of Ogunlana (2019), who highlighted reasons why Nigeria is finding it difficult to counter terrorism activities on the Internet. Weak leadership, nepotism, corruption, and a lack of technological expertise have continued to plague the agencies responsible for security in Nigeria. Results obtained from literature is in consistent with results obtained from the field. All the interviewees' interviewed responded that the Nigerian security structure is not capable to counter online radicalisation of lone wolf terrorist. Even though, majority of them mentioned that by de-radicalising potential radicals remain the best approach to counter lone wolves terrorist due to its preventive style and the long-term effect it will have on the Nigerian security situation. Such de-radicalisation approaches may involve the engagement of stakeholders in the education sector, faith-based organisations, and the health sector.

6.0 Conclusion

The Internet is now the new war ground for terrorism. Social media platforms like YouTube, Twitter, and websites affiliated with terrorist organisations have become primary channels for extremist propaganda. The ease of access and anonymity offered by the internet empowers individuals to explore extremist ideologies and radicalise lone wolves. The internet plays a significant role in facilitating the self-radicalisation of lone wolf terrorists by offering a platform for connection, anonymity, exposure to extremist content, and access to radical materials. These findings highlight the urgent need for multifaceted counter-terrorism strategies. While Western nations have implemented some measures like electronic surveillance and community engagement programmes, Nigeria's efforts seem inadequate due to her deficiency in technological expertise and her reliance on de-radicalisation approaches offline.

7.0 Recommendations

1. Social media platforms like YouTube, Twitter, and Facebook should be pressured to increase restrictions on extremist content. This could involve implementing better algorithms to detect and remove extremist videos and posts, and cooperating with law enforcement to identify and disable accounts linked to terrorist organisations.

2. Governments and civil society organisations can create online campaigns that challenge extremist narratives and promote peace and tolerance. These campaigns could be targeted at specific demographics or communities that are vulnerable to radicalisation.

3. Government should collaborate with relevant stakeholders on ways of engaging communities through the use of educational programmes. Educational programmes can be developed to teach people about the dangers of extremism and how to identify extremist propaganda online. These programs could be targeted at young people, religious leaders, and community leaders. Programmes like this can help people who have already been radicalised to disengage from extremist ideologies. These programmes could involve religious counseling, social support, and job training.

4. Since the new battlefield is now the internet, Nigerian law enforcement agencies should use electronic surveillance techniques to monitor online activity and identify potential lone wolves. However, it is important to balance these measures with privacy concerns. On this note, Nigeria needs to invest in developing the technical expertise to counter online terrorism. This could involve training law enforcement officials and cybersecurity experts in how to identify and dismantle terrorist websites.

5. There is also need for international cooperation in the fight for curbing the activities of extremist groups on the internet. This is because, international cooperation is essential to counter online terrorism. Countries need to share information about terrorist threats and work together to develop effective counter-terrorism strategies.

References

ABC. (2015, May 7). Canada passes new anti-terrorism law expanding spy agency powers. *ABC News*, p. 1.

Alfaro-Gonzales, Lydia, et al. (2015). *Report: Lone Wolf Terrorism*. Washington, DC: Georgetown University.

Alim, S., Hassan, G., & Schroeder, H. (2018). Countering online violent extremism: A review of government and technology company initiatives. *International Journal of Communication*, 12(2), 1204-1231.

Arts, L., & Butter, E. (2009). Radicaal, orthodox, of extremist? Achtergrondinformatie over radicalisering en polarisatie. Amsterdam: ABC Kenniscentrum voor Emancipatie en Participatie.

Asemah, E.S. (2011). *Mass Media in the Contemporary Society*. Jos: Jos University Press Limited

Bakker, J., De Vreese, A., & Edgerly, C. (2018). The spread of online misinformation: Why echo chambers are not enough. *European Journal of Communication*, 33(2), 187-207.

Benson, D.C. (2014). Why the internet is not increasing terrorism. *Journal of Security Studies 23*, 293–328. https://doi.org/10.1080/09636412.2 014.905353.

Berg, B.L. (2012). *Qualitative Research Methods for the Social Science*. Long Beach: Allyn and Bacon, 8.edition.

Berghuijs, M., & Hopkins, N. (2019). The role of online social identity in (counter)

Bergin, A., Osman, S., Ungerer, C., & Yasin, N. (2009). Countering internet radicalisation in Southeast Asia. *Australian Strategic Policy Insitute Special Report*, (22).

Bergsen, T., & Bjørgo, T. (2015). Vulnerability to radicalization: A social psychological perspective. *Journal of Deradicalization, 4*(1), 122-144.

Borum, R. (2011). Radicalization into violent extremism: A review of social science theories. *Journal of Strategic Security*, *4*(4), 7–36. https://doi.org/10.5038/1944-0472.4.4.1

Boyd, D. M. (2008). Why youth love social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity and digital media*. (pp. 119–142). Cambridge: The MIT Press.

Brachman, Jarret. M. 2006*. "High-tech terror: Al-Qaeda's use of new technology."* Manuscript submitted for publication, Combating Terrorism Center, United States Military Academy, Lincoln Hall, New York

Brandon, J., 2008. *Virtual Caliphate Islamic extremists and their websites*. London: Published by Centre for Social Cohesion.

Byford, J. (2017). Understanding recruitment and radicalization: A critical review of key theories. *Studies in Conflict & Terrorism, 40*(11), 943-963.

Chrisafis, A. (2015, May 5). France passes new surveillance law in wake of Charlie Hebdo attack. *The Guardian*, p. 1.

Cohen, K., Johansson, F., Kaati, L. & Mork, J.C. (2014). Detecting linguistic markers for radical violence in social media. *Journal of Terrorism and Political Violence 26*, 246–256. https://doi.org/10.1080/09546553.2014.849948

Conway, M. (2012). From al-Zarqawi to al-Awlaki: The emergence of the internet as a new form of violent radical milieu. *Combating Terrorism Exchange*, *2*(4), 12–22.

Coulombre, J.W. (2021). *Trends of terrorism activity in relation to internet accessability throughout the Sahel countries of Africa*. Retrieved from https://jscholarship.library.jhu.edu/server/api/core/bitstreams/ba5c4b25-d4ba-4548-8d2a-4a6a9c099f1a/content.

Freiburger, T. & Crane, J.S. (2008). A systematic examination of terrorist use of the internet." *International Journal of Cyber Criminology*, *2*(1), 309-319.

Gebhard, J., Weikert, R., & Küpper, S. (2019). The role of emotions in radicalization: A review of the literature. *European Journal of Social Psychology*, *49*(2), 443-460.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. & Horgan, J. (2017). Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology & Public Policy, 16*, 99–117. https://doi.org/10.1111/1745-9133.12249

Greenberg, K. (2016). Counter-radicalization via the internet. *Annals of the Academy of Political and Social Sciences*, *668*, 167-179.

Grubb, B. (2014, September 25). Terror laws clear Senate, enabling entire Australian web to be monitored and whistleblowers to be jailed. *The Sydney Morning Herald*, p. 1

Guri, N.M. & Ravndal, J.A. (2021). Mechanisms of online radicalisation: How the internet affects the radicalisation of extreme-right lone actor terrorists. *Behavioral Sciences of Terrorism and Political Aggression*, doi: 10.1080/19434472.2021.1993302.

Hafez, M., & Mullins, C. (2015). The radicalization puzzle: A theoretical synthesis of empirical approaches to homegrown extremism. *Studies in Conflict & Terrorism*, *38*(11), 958-975.

Hennigan, W.J. (2018). *How big a role does social media play in homegrown terrorism?* Retrieved from https://time.com/5438481/terrorism-social-media/

Jenkins, B.M. (2010). Would-be warriors: Incidents of jihadist terrorist radicalization in the United States September 11, 2001." *Testimonial, RAND Corporation*.

Jenkins, B.M. (2011). Jihadist use of social media: How to prevent terrorism and preserve innovation." *Testimonial, Committee on Homeland Security and House of Representatives*.

Kalyuzhnova, Y., Hodges, J., & Lester, W. (2018). The role of the online environment in radicalization. *International Review of Counterterrorism*, *9*(2), 161-176.

Klausen, J. (2015). Tweeting the jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, *38*(1), 1-22.

Klausen, J., Barbieri, E.T., Reichlin-Melnick, A. & Zelin, A.Y. (2012). The YouTube jihadists: A social network analysis of Al-Muhajiroun's propaganda campaign. *Perspectives on Terrorism*, *6*(1).

Koehler, D. (2014). The radical online: Individual radicalization processes and the role of the internet. *Journal for Deradicalization*, *1*, 116–134.

Malthaner, S., & Lindekilde, L. (2017). Analyzing pathways of lone-actor radicalization: A relational approach. In M. Stohl, R. Burchill, & S. Englund (Eds.), *Constructions of Terrorism*, 163–180. University of California Press.

Marcks, S., & Pawelz, S. (2020). *The new digital jihad: Global networks of extremist salafists in the online sphere*. Rowman & Littlefield.

Maréchal, L., Girard, S., & Lefebvre, G. (2019). Countering violent extremism narratives: A critical review of online interventions. *Studies in Conflict & Terrorism*, *42*(7), 580-600.

McCauley, C., & Moskalenko, S. (2008). Mechanisms of political radicalization: Pathways toward terrorism. *Terrorism and Political Violence*, 20(3), 415-433.

McCauley, C., & Moskalenko, S. (2008). Mechanisms of political radicalization: Pathways toward terrorism. *Terrorism and Political Violence*, 20(3), 415-433.

McCauley, C., & Moskos, C. C. (2008). *Extremists in the digital age*. Cambridge University Press.

McDowell-Smith, A., Speckhard, A., & Yayla, A. (2017). Beating ISIS in the digital space: Focus testing ISIS defector counter-narrative videos with American college students. *Journal for Deradicalization*, 10, 50-76.

Meehan, J., Atran, S., & Axelrod, R. (2011). The ISIS paradox. *Studies in Conflict & Terrorism*, *34*(9), 709-728.

Meloy, J.R. & O'Toole, M.E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences & the Law* 29: 513–527. https:// doi.org/10.1002/bsl.986

Mueller, J. & Stewart, M.G. (2015). Terrorism, counterterrorism, and the Internet: The American cases. *Dynamics of Asymmetric Conflict* 8: 176–190. https://doi.org/10.1080/17467586.2015.1065077

Neo, L. S. (2016). An internet-mediated pathway for online radicalisation: *RECRO. In M. Kader, L. S. Neo, G. Ong, E. T. Mingyi, & J. Chin.* 197–224. https://doi.org/10.4018/978-1-5225-0156-5.ch011.

Neumann, P. R. (2011). *Preventing violent radicalization in America*. (Policy Report). Washington, D.C.: Bipartisan Policy Center.

Ogunlana, O. F. (2019). Determinants of public sector corruption in Nigeria. *International Journal of Public Policy and Administration Research*, *6* (1), 1-11.

Olivier, R. (2015). Boko Haram: A rebellion within a rebellion. *International Affairs*, *91*(2), 397-414.

Pantucci, R. (2011). A typology of lone wolves: Preliminary analysis of lone islamist terrorists. *Developments in Radicalisation and Political Violence*, 1-39.

Sageman, M. (2008). The next generation of terror. *Foreign Policy*, *165*, 37.

Scrivens, R., Davies, G. & Frank, R. (2018). Searching for signs of extremism on the web: an introduction to Sentiment-based Identification of radical authors. *Behavioral Sciences of Terrorism and Political Aggression*, *10*(1), 1–21. https://doi.org/10.1080/19434472.20 16.1276612.

Silber, M., & Bhatt, A. (2007). *Radicalization in the West: The homegrown threat.* New York: New York City Police Department.

Sirkku, J. (2016). Online radicalization and violent extremism. *The RUSI Journal*, *161(*2), 24-34.

Špiláčková, M. (2012). Historical research in social work: Theory and practice. *ERIS Web Journal, Volume 3* (2), 22-33

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. *European Journal of Social Psychology*, *9*(4), 143-170.

Theohary, C.A. & Rollins, J. (2011). *Terrorist use of the internet: Information operations in cyberspace.* http://www.fas.org/sgp/crs/terror/R41674.pdf.

Thompson, R. (2011). Radicalization and the use of social media. *Journal of Strategic Security. 4*(4), 167-190.

Torok, R. (2010). Make a bomb in your mums kitchen: Cyber recruiting and socialisation of 'White Moors' and 'Home Grown Jihadists'. Paper presented at the Australian Counter Terrorism Conference., Pert Western Australia.

Torok, R. (2013). Developing an explanatory model for the process of online radicalisation and terrorism. *Security Informatics, 2*(1), 6. https://doi.org/10.1186/2190-8532-2-6.

Transnational Terrorism, Security & the Rule of Law (2008). Causal factors of radicalisation. Retrieved from http://www.transnationalterrorism.eu/tekst/publications/Causal%20Factors.pdf

Tsfati, Y. & Weimann, G. (2002). *Terror on the internet*. *Studies in Conflict & Terrorism*, *731*, 317–332. https://doi. org/10.1080/1057610029010121.

United Nations Office on Drugs and Crime (UNODC) (2012). *The use of the Internet for terrorist purposes.*United States Institute of Peace. Washington D.C. http://www.usip.org/files/resources/sr116.pdf.

Van de Linde, E., & Rademaker, P. (2010). Een toekomstverkenning van de invloed van brede maatschappelijke trends op radicaliseringsprocessen. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum

von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the digital era* RAND. https://www.rand.org/pubs/research_reports/RR453.html.

Wagenaar, W. (2010). Extreemrechtse formaties. In P. R. Rodrigues & J. Donselaar (Eds.), *Monitor Racisme en Extremisme: Negende rapportage*. (pp. 37–62). Amsterdam: Anne Frank Stichting/Universiteit Leiden

Weimann, G. (2005). How modern terrorist use the internet. *The Journal of International Security Affairs.*

Weimann, G. (2010). Terror on Facebook, Twitter, YouTube. *Brown Journal of World Affairs*, *16*(1), 45-54.

Weimann, G. (2011). *Al qaeda has sent you a friend request: Terrorists using online social networking.* Manuscript submitted for publication, Communication, Haifa University, Israel.

Weimann, G., & Von Knop, K. (2008). Applying the notion of noise to countering online terrorism. *Studies in Conflict & Terrorism*, *31*(10), 883–902. https://doi.org/10.1080/10576100802342601.

Woodring, D.W. (2014). *21st century radicalization: The role of the internet user and nonuser in terrorist outcomes* [Doctoral thesis, University of Arkansas, Fayetteville] http://scholarworks.uark.edu/etd/2338

Wray, C. (2020). *Statement made before the house judiciary committee Washington, D.C.* Retrieved from https://www.npr.org/2017/12/07/568611745/fbi-director-wray-testifies-before-house-judiciary-committee

Yeap, S.Y. & Jenna, P. (2010). Countering internet radicalisation: A holistic approach'. *S. Rajaratnam School of International Studies* http://dr.ntu.edu.sg/bitstream/handle/10220/6657/RSIS0782010.pdf?sequence=1