View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

Ann. Disaster Risk Sci. 2018, 1, 27-33

NEW SECURITY PARADIGM – THE USE OF SOCIAL NETWORKS AS A FORM OF THREAT TO THE NATIONAL SECURITY STATE

Khulood Ali Jumah Al Jarman Al Zaabi[1], Duško Tomić[2]

[1]American University of Emirates in Dubai, United Arab Emirates
[2]American University of Emirates in Dubai, Faculty for security and global studies, United Arab Emirates

Abstract

Islamic State depends on the recruitment of foreign fighters to execute attacks in their home countries. This paper examines the influence of social networks such as Facebook, Twitter, and YouTube in the indoctrination and direction of young people into extremist and terrorist collectives. The study wholly depended on the qualitative analysis in unfolding the concerns related to social media and terrorism activities. After an in-depth exploration, the paper has proven that a good number of attacks are launched by homegrown terrorists who are self-radicalized and indoctrinated through YouTube videos, Facebook groups, and Tweets. Following this discovery, the researchers recommend collaboration between the social media owners and intelligence security agencies in combating terrorist activities online. The social media owners' help in monitoring terrorists' activities on their websites would thus help in improving the intelligence and the general security of the country.

Keywords: Radicalization, Social Media, ISIS, Al-Shabaab, Facebook, Twitter.

Adress for correspondence: Khulood Ali Jumah Al Jarman Al Zaabi, American University in the Emirates, Dubai, United Arab Emirates, e-mail: K.alzaabi12@hotmail.com.

1. INTRODUCTION

The current social media platforms completely differ from the traditional media channels in numerous ways. This provides a good ground for the terrorists to create their own channels, reach a huge audience and circulate their messages globally [1]. Furthermore, it gives them a platform to ensure that their propaganda remains live forever in online environment. A unique property and feature of social media is that it is very democratic in the sense that it gives everyone an opportunity to publish and easily access information online [2]. In contemporary world, social media has been used in inciting fear and delivering threats (Tweets) to the general public [3]. Furthermore, it is used in radicalizing others, creating a sense of terrorist community, romanticizing the Islamic State [IS] and Sharia law and offering logistics and travel advisory to their new recruits [4]. A good example of a social media influenced terrorist attack is the Orlando nightclub attack by Omar Mateen. The attack left 49 people dead and scores of those injured [5].

According to the report by the Homeland Security Digital Library titled "Jihad 2:0", terrorist groups such as Al-Qaeda, Islamic State of Iraq and Syria [ISIS], and Al Shabaab located in Arabian countries are using social media to spread their online propaganda and recruit extremists in the United States of America [6]. ISIS has been using social media gateways such as Twitter, Facebook, Google, and other popular services, including YouTube, WhatsApp, Skype, and Instagram to lure most Western recruits to Syria for terrorist training [2]. Basically, the new tactic of using social media brings the notion that a country should not only depend on the military force in eliminating terrorist threats but they should also work closely with the Siren Servers such as social media platforms in examining and monitoring any terrorist activity around the globe. Countries or parties touched by this issue include African countries, Syria, Yemen, Turkey and the United States of America [4]. Bearing these facts in mind, it is important to evaluate the political, legal and operational reasons why this indoctrination occurs.

Terrorism makes a country's politics difficult and complicated to handle. For instance, between April 2013 [when the Boston Marathon Attack occurred] to now, the United States have faced 13 terrorist attacks from individuals who are self-radicalized through the use of online jihadist propaganda and mosque ties to the ISIS, Al-Shabaab or the Al-Qaeda. Fundamentally, these attacks leave the United States without a clear enemy to attack. After the Orlando nightclub attack, President Obama termed it to be a homegrown terrorist who was inspired by numerous radical jihadist materials available on the Internet [social media]. The Orlando nightclub attack looked similar to the shooting which occurred at San Bernardino in 2015 that left 14 people dead [5]. Therefore, the primary terrorist focus is destabilizing the politics of the country by creating distrust among the political leaders in order to take control of the government, its people, and resources.

According to public law, international terrorism is a dangerous or violent act to the human life and which violates the criminal law as stipulated by the United States constitution or any other state [4]. In the USA, violation of human life through terrorism is considered a criminal activity by the legal system if it is committed within the jurisdictions of the United States. Public law states that terrorist acts happen in order to intimidate a civilian population, influence certain governmental policies through coercion and intimidation and affect the conduct of ruling governments through kidnapping, mass destruction, and assassinations. These have been evident in Chattanooga, Tennessee on July 16, 2015, when Muhammad Youssef Abdulazeez killed a sailor and four marines at a military base located in Chattanooga. Duplicate events happened in San Bernardino, Garland Texas, and Queens in New York. In all these attacks, civilians are intimidated and influenced through fear [7].

Initially, the government relied on the military force to eject terrorist groups from their hideouts in Syria and Iran. But at the moment ISIS and other terrorist groups have changed their tactics in recruiting and launching their attacks. They are using social media to recruit, as well as to assign missions to their new recruits. After the attack, they again use the same social media platforms to claim responsibility [2]. According to James Comey, the former FBI director, some of the youths and teens in the United States have been radicalized after consuming a dangerous poison on the Internet. This "dangerous poison" is the indoctrination happening on the social media where operations are planned, recorded live and the responsibility for the attacks announced immediately by their leaders.

Over the last few years, the United States of America have suffered numerous threats and terrorist attacks by radical Islamic terror groups. Attempts to discover lone terrorists or attack terrorist hideouts have not had any effect on the alleviation of terrorist attacks as well as the pain suffered by many Americans at the hands of jihadists, Al-Qaeda and Al-Shabaab. From the year 2013, terrorist groups under the direction of foreign terror organizations and leaders have taken social media as the new breeding environment for new recruits and distribution of online terror propaganda [4].

2. METHODOLOGICAL APPROACH

Data and information for this research paper were gathered through the use of ISIS, social media & terrorism, online indoctrination of terrorists and self-radicalization as the main keywords and key search terms in order to obtain qualitative data on the topic. Based on the information and ideas obtained, the quality, utility, and relevance of the materials have proven to be excellent as the corpus of materials has yielded an abundance of information that has helped in examining the arguments presented in the paper. The paper relied on intensive analysis to pick out specific ideas and information relevant to the research topic.

3. SECURITY ANALYSIS OF SOCIAL MEDIA

The Homeland Security Department [HSD] and the Federal Bureau of Investigation [FBI] un-

der James Comey used the Social Network Analysis to connect dots and gather intelligence in fighting terrorism [8]. They applied public information, hints given by newspapers and open source data to check and evaluate instances of threats or pre-planned attacks in the United States [3]. Furthermore, they worked closely with social media companies such as Facebook and Twitter to release information, phone numbers and exact locations where some tweets, messages, webinars or videos were uploaded. Additionally, they evaluated groups, terrorist keywords, and movements created on these platforms with the aim of spreading fear or propaganda online [2]. To access these accounts, a security agent can simply look for links on YouTube, Twitter, and Facebook with keywords such as radical use or ISIS.

4. METHODS OF TRAINING

Online indoctrination of terrorist recruits is a complex process that involves tedious engagement of the new catch with the massive amount of online propaganda. Naturally, terrorists present their online propaganda materials online through social media platforms such as Facebook, Twitter, and YouTube videos [1]. In these online spaces, terrorists use a technique called future pacing where they challenge existing religious beliefs such as the oneness of God, abhorrence of idols and Catholicism [2]. By placing these innocent foundations, they slowly plant a seed about the active differences and injustices faced by fellow Muslims. The core aim is creating a belief that all other religions are against them and therefore they must use violence to emphasize their presence [4].

5. POSSIBLE SYSTEMS OF DEFENSE AND CONTROL OVER SOCIAL NETWORKS

According to Computer Emergency Response Team, immediately after recruitment, ISIS recruiters shift their communications to private. They do this through encrypted messaging platforms where no third parties can access the information passed. Therefore, the Homeland Security Department, CIA, and FBI may invest in secure hardware and software that easily detects ISIS or radical keywords hence blocking their access immediately [3]. Another effective way is affiliating with the social media account owners for the easy tracking of threats. With this public and private partnership, security agents can easily detect and capture any terrorist group running or recruiting members on social media [9].

6. EXCHANGE OF INFORMATION BETWEEN INTELLIGENCE UNITS

Though the French intelligence agencies have been accused of failure that led to the Paris attacks, the experience presents numerous methods through which intelligence information is passed from one intelligence unit to another. According to James Comey, the former FBI director, most of the terrorist communications have gone dark and therefore it is important for intelligence agencies to pass their intelligence information through encrypted e-mails, messages and phone records other than using public networks and the word of mouth as experienced in Paris before the attacks [4]. Basically, good cooperation between intelligence services may help in sharing relevant information without risking the leaking of intelligence information. For example, the lack of cooperation between the French and Turkish governments on the issue concerning Mostefai, where some attackers were believed to be hiding, exposed Paris to the deadly attacks [9].

7. INDOCTRINATION OF INDEPENDENT OPERATING INDIVIDUALS

As highlighted above, terrorist organizations and groups are recruiting both groups and independent individuals around the world. In the United States, such individuals are referred to as homegrown terrorists or self-radicalized terrorists [2]. Independent terrorists are indoctrinated using online jihadist propaganda and live Al-Qaeda teaching through the use of YouTube and webinar videos. Good examples are Tamerlan and Dzhokhar Tsar-

naev who placed two bombs during the 2013 Boston Marathon. The attack left six people dead and 260 fatally injured. According to FBI reports, these two Tsarnaev brothers were self-radicalized terrorists who were recruited into jihadi circles through online media and YouTube videos on jihadist topics and the sharia law.

Also, on September 24, 2014, in the town of Moore in Oklahoma, a terrorist by the name Alton Nolen beheaded Colleen Huff and stabbed another individual at Vaughan Foods Plant. After an investigation, it was proven that Alton was radicalized through Facebook and Twitter. Moreover, on October 23, 2014, in the Queens borough of New York, Zale Thompson, a social media indoctrinated terrorist, injured two police offers using a hatchet before getting shot by the patrol policemen [3]. The same scene was repeated on December 20, 2014, in Brooklyn in New York after Ismaaiyl Brinsley killed two police offices in an execution style [7]. In essence, most terrorist groups are using social media as their main breeding grounds for hunting and training their new recruits. They mainly target American teens and Middle Eastern immigrants in developing countries to launch their new attacks. Terrorist recruiters send numerous messages to the so-called non-believers as a way of intimidating them and expressing their assumed injustices to the Muslim society. They do this by discussing issues related to Catholicism and how the inability to control similar religions would lead to the end of the Muslim population. The sharing of intelligence information among security agents is very important as it helps in preventing possible attacks. To highlight this issue one may mention how before the Paris attacks Belgium and Turkey tried to share certain intelligence with the French intelligence agencies, but they declined to take it seriously. As a result, the very same information they were being offered ended up affecting them.

8. PREVENTION SYSTEM

Online indoctrination of individuals can only be controlled by investing in software that detects and deletes radical keywords on social media groups. According to Naco (2016), individuals should keep calm during such risky situations and report any suspicious information either by pressing the report content button on Facebook or by reporting it to a security agent [9].

Furthermore, the researchers attempt to predict the terrorists' and other groups' future behavior by observing their activities while organizing themselves using social media, and then gathering the data observed to create predictive algorithms that could be used as anti-terrorism tools [10].

9. STATEMENT

According to the Homeland Security Department, terrorism has changed gears in this new era of social media. Propaganda, recruitment, and training are currently done online, while camouflaging as religious training groups. Over the last few years, a massive number of Americans have lost their lives through such attacks. While explaining the relationship between social media indoctrination and terrorism, the Orlando and San Bernardino attacks can serve as good examples of the cost of social media indoctrination of youths into terrorism [9]. The literature review has also provided an in-depth exploration of how and who are recruited by these online terrorist agents.

10. ARGUMENT

This study argues that most terrorist attacks committed by young offenders, whether independently or in groups, are linked to social media. Furthermore, it presents the fact that social media is used as a platform for spreading jihadist propaganda, recruitment, training and planning of domestic terrorist attacks.

11. DESCRIPTION OF THE TERRORIST USE OF SOCIAL MEDIA AGAINST NATIONAL SECURITY

According to the FBI, the Orlando nightclub attack was committed by an American-born man who was linked to the ISIS. After the operation and

investigation, Omar Mateen was labeled as the main suspect who committed the attack [5]. He also helped in mentioning the Boston Marathon bombers. As a homegrown terrorist who was indoctrinated through Facebook, Omar Mateen killed 49 people and injured scores of others. In this case, the legal aspects of the UN Charter only worked in highlighting the inhuman activities committed by this terrorist. However, the primary investigation was under the purview of the FBI who arrested all individuals related to the crime, including Omar's wife Noor Salman. In essence, social media has helped in the recruitment and training of many young people in the United States who subsequently become the enemies of progress.

12. ANALYSIS OF THE TERRORIST USE OF SOCIAL MEDIA AGAINST NATIONAL SECURITY

Initially, security agencies such as the FBI, the Homeland Security and other international intelligence agencies have been relying on military forces to eject terrorists from their hideouts. In contemporary times, terrorism has taken a new shape where every activity is planned online through the use of social media and the dark web [2]. This presents the main challenge why intelligence is failing in capturing some of the most important information being passed from one terrorist agent to another. These fails in the intelligence coordination have been present during the Istanbul attack, the Paris attack, the Berlin attack and the Orlando attack where homegrown individuals were acting as the primary enemies of their nations [9].

The actions launched by terrorist groups are not ethical as they cause the destruction of property, injury to people, as well as loss of life. For example, in the San Bernardino case in December 2015, more than 15 innocent lives were lost with a massive number of additional injuries. On the contrary, the operations implemented by the Homeland Security Department and the FBI are very ethical as they are determined to achieve peace and security in the country. Over the last few years, many terrorists have been caught and charged before the court of law [8].

As highlighted in the literature review, terrorist attacks are aimed at intimidating political powers in the affected countries. They do so by inciting fear among the general public in order to cause conflict between them and their leaders and governments. Terrorists argue that these nations inhumanly kill their Muslim brothers and sisters and therefore revenge is justified for their behavior. In all cases involving terrorist attacks mentioned, James Comey, the former director of the FBI remained the primary decision maker who approved the missions to investigate different types of criminal activities either online of offline [9].

In this case, the FBI and the Homeland Security Department are the primary actors in preventing any terrorist attacks either online or physically. They apply technology in order to detect and evaluate terrorist activities and interview sympathizers who may help with information related to terrorist plans. In all cases, operations executed by the FBI and the Department of Homeland Security have brought all suspects and criminals to book. For example, in the case of San Bernardino, Tashfeen Malik and Syed Farook were arrested [7]. Omar Mateen was arrested in relation to the Orlando nightclub attack, while Dahir Ahmed Adan was arrested in relation to the St. Cloud attack in Minnesota. In essence, every operation implemented by the security agents ended up yielding actual information and other intelligence data related to other planned attacks.

Following their research, the authors feel that the Department of Homeland Security is doing a great job in maintaining the security of the United States of America. Furthermore, it is important to work closely with Facebook and Twitter in order to detect and prevent criminal activities before they are committed [8]. Finally, the FBI should work closely and in cooperation with other intelligence agencies internationally in order to maintain control over all information and activities of terror groups.

13. RECOMMENDATIONS

Based on the fact that terrorism has implemented a new strategy in planning and recruiting people, Naco (2016) suggests that international intelligence agencies should work together to achieve a holistic security platform that screens and monitors online activities from all over the world [9]. Moreover, security agencies such as the FBI and the Homeland Security Department should establish partnership with the social media owners in order to implement an intelligent system that screens, detects and deletes all radical information from their websites.

Also, security agencies' role includes conducting covert operations related to the development, surveillance, and analysis of social media with the purpose of attracting any current and potential jihadists who intend to search for forums that contain conversations related to terrorism or criminal activities that might cause threats to the national security and the safety of their populations. Terrorist attacks may be prevented by establishing cooperation between the government agencies and the private sector responsible for combating cyber-threats, as well as through the development of cyber security policies and by raising public awareness to safeguard national security [11].

Data protection and privacy policies related to the Internet and digital personal data ought to be maintained. These policies aid the smartphones and Internet users while reporting any violence or politically sensitive issues. Security officers should be educated and trained on social media guidance and its applications in a periodic manner, in order to defend against any social media issues such as privacy and political issues.

In addition, security apparatus should be developed that aims to gather and analyze the social media data automatically against this type of terrorist activities. Furthermore, a research community specialized in this area should be brought together; amplifying strategic communication and social media presence in order to thwart any terrorist activities such as propaganda by weakening the extremists' credibility.

14. CONCLUSION

Following our research, it is evident that social media can be directly linked to terrorism planning, recruitment, and attacks. Many terrorist groups use the available social media platforms to spread their jihadist propaganda, report on incidents, as well as train homegrown terrorists in various countries [9].

14.1. Outcomes

The overall outcome of increased indoctrination of individuals through the use of social media has resulted in an increased number of youngsters who joined these groups. As a result, the lack of security has tripled in the world, the United States being the most affected by this. Additionally, more lives have been lost following an increase in terrorist attacks in the country.

14.2. Concluding Remarks

Based on the growing number of technological innovations and the growth of social media platforms that are connecting the world, any future research should look into technologies that can be used in controlling terrorist activities on social media platforms. Any future researcher must therefore understand that 90% of terrorist activities have gone dark, meaning that it is high time to research the strategies to control their clandestine activities.

15. REFERENCES

1. Taylor, H. (2016). "Most Young Terrorist Recruitment Is Linked To Social Media, DOJ Official Says", CNBC, accessed February 21, 2017, URL: http://www.cnbc.com/2016/10/05/most-young-terrorist-recruitment-is-linked-to-social-media-said-doj-official.html.
2. Bennett, D. (2013). Digital media and reporting conflict: blogging and the BBC's coverage of war and terrorism. New York: Routledge.
3. Alarid, M. (2016). "CHAPTER 13 Recruitment And Radicalization: The Role Of Social Media An", Center For Complex Operations, accessed February 21, 2017, URL: http://cco.ndu.edu/Publications/Books/Impunity/Article/780274/chapter-13-recruitment-and-radicalization-the-role-of-social-media-and-new-tech/.
4. WIRED. (2016). "Why ISIS Is Winning The Social Media War—And How To Fight Back", accessed February 21, 2017, URL: https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.
5. Lohrmann, D. (2016). "How Terrorists' Use Of Social Media Points To The Future", Govtech.Com, accessed February 21, 2017, URL: http://www.govtech.com/em/safety/Terrorists-And-Social-Media.html.
6. Rowland, M. (2017). "Jihad 2.0: The Power Of Social Media In Terrorist Recruitment – Homeland Security Digital Library", Hsdl.Org, accessed February 21, 2017, URL: https://www.hsdl.org/c/jihad-2-0-the- power-of-social-media-in-terrorist-recruitment/.
7. Barrett, J. (2017). "A Complete List Of Radical Islamic Terror Attacks On U.S. Soil Under Obama", Daily Wire, accessed February 21, 2017, URL: http://www.dailywire.com/news/11410/complete-list-radical-islamic-terror-attacks-us-james-barrett.
8. Steinbach, M. (2016). "ISIL Online: Countering Terrorist Radicalization And Recruitment On The Internet And Social Media", Federal Bureau Of Investigation, accessed February 21, 2017, URL:https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media.
9. Nacos, B. L. (2016). Terrorism and Counterterrorism. New York : Routledge, Taylor & Francis Group.
10. Caruso, C. (2016). "Can a Social-Media Algorithm Predict a Terror Attack?" MIT Technology Review. URL: https://www.technologyreview.com/s/601700/can-a-social-media-algorithm-predict-a- terror-attack/.
11. Kimutai, J. (2014). "Social Media and National Security Threats: A Case Study of Kenya." Master's thesis, University of Nairobi. URL: http://erepository.uonbi.ac.ke/handle/11295/76667.

NOVA SIGURNOSNA PARADIGMA – KORIŠTENJE SOCIJALNIH MREŽA KAO OBLIK UGROZE NACIONALNE SIGURNOSTI

Sažetak

Islamska država ovisi o regrutiranju stranih boraca za izvršenja napada u njihovim matičnim zemljama. Ovaj rad istražuje utjecaj društvenih mreža kao što su Facebook, Twitter i YouTube u indoktriniranju i usmjeravanju mladih ljudi u ekstremističke i terorističke kolektive. Studija je u potpunosti ovisila o kvalitativnoj analizi vezano za problem društvenih medija i terorističke aktivnosti. Nakon iscrpnog istraživanja, document je dokazao da velik broj napada pokreću domaći teroristi koji su samoradikalizirani i indoktrinirani kroz YouTube, Facebook grupe i Twitter. Nakon ovog otkrića, istraživač je preporučio suradnju između vlasnika društvenih medija i sigurnosno-obavještajnih agencija u borbi protiv terorističkih aktivnosti na internetu. Vlasnici društvenih medija pomoći će u praćenju aktivnosti terorista na svojim web stranicama što će poboljšati obavještajne aktivnosti i opću sigurnost zemlje.

Ključne riječi: radikalizacija, društveni mediji, ISIS, Al-Shabaab, Facebook, Twitter.