Chapter 3

Retweeting Radicalization: Radicalization and Recruitment to Terrorist Organizations in the Information Age

Nicole Wojtkiewicz

Abstract

In a time of technological advancement and media domination, terrorist organizations are evolving their means of recruitment and radicalization. It is imperative that an accurate light is shed on this phenomenon. This article aims to explain how Jihadist terrorists and terrorist organizations are utilizing technological advancements, like social media, in their recruitment tactics. It is important to define what is meant by information age, radicalization, and recruitment as it relates to the research conducted. There appears to be a lack of research, consensus, and understanding pertaining to actual social media usage and effects by these organizations. Drawing from varying perspectives, research, and studies, what is occurring through Internet sites like Twitter, Facebook, and YouTube, and the realistic threats that this usage is posing will be examined. In an effort to alleviate misunderstandings and disproportionate reactions, the article will outline practical counter efforts that can be deployed to combat these ever-evolving recruitment tactics. Finally, certain criticisms and limitations pertaining to research, policies, and misinformation are pointed out. All the information outlined leads to the concluding notion that although an effective aid in recruitment tactics, Internet and social media use is not alone enough to create a terrorist.

Introduction

In a time referred to as the "information age", "digital age" or the "media age" there has been much speculation concerning the role of technological advancements and its aid to terrorist organizations; specifically speaking, the ability to utilize things such as the Internet and global communities to recruit and radicalize for the organization. When referring to the Information age, this article utilizes Manuel Castells (2010) ideas concerning the rise of a network society. This refers to a period in the 2nd millennium. During this time the world experienced social, technological, economic shifts altering society into a modern network society. A focus of this article consists of communication shifts from traditional mass media to a more decentralized and horizontal society surrounding the Internet. This allows new means of varied and efficient communications (Castells, 2010, pp. 17–18). Terrorists no longer must solely rely on the media and news networks to spread their propaganda, attacks, and fear. They now possess the tools to spread their messages themselves through online networks with social media platforms, but what is it exactly that terrorist organizations are trying to spread and accomplish through their use of the internet?

What is clearly of most concern is terrorist organizations modern ability to radicalize and recruit efficiently through social media. The terms radicalize and recruit will be used in this paper in similar contexts. By recruit is defined as convincing someone to join a cause. When discussing radicalization throughout this paper, it will refer to Chatfield et. al., (2015) interpretation as

> 'Increasing extremity of beliefs, feelings, and behaviors in support of political violence in a context of strong group identification and response to perceived threat to the in-group' (p. 7).

An observable and possibly obvious pattern, that should be understood to follow this paper is the necessity of radicalization to recruit people to terrorist organizations.

With this basic background knowledge, the paper will continue to observe the ways that the Internet is exploited by terrorists and organizations and how this is built off their traditional recruitment methods. Next, the actual threats that this Internet is posing and its implications are highlighted. Following this, practical steps as to how to combat the ever-evolving use of the Internet to radicalize and recruit to illicit organizations will be outlined. Once the use, threats, and solutions of this Internet use are explained, this paper points out limitations and criticisms concerning studies, public opinion, and policies regarding Internet use by terrorist organizations. This all adds up to the concluding point that the Internet can influence radicalization and recruitment, but it alone cannot create a terrorist.

How the Internet is Actually Utilized by Terrorist/ Jihadist Organizations

Social media platforms have freed terrorist organizations like Al Qaeda and the Islamic State of Iraq and Syria (ISIS) from relying on mainstream media to communicate and disseminate information. They would normally have to rely on dramatic events and threats to be picked up by news outlets. This would then spread their messages and their so-called victories. Now anyone can participate. The fact that social media, blogs, and file sharing apps are low cost, quick, and anonymous, they are able to reach greater audiences efficiently (Klausen, 2015, p. 4). There seems to be a misconception concerning what and how terror organizations are using these social media platforms. From analyzing several studies, the author has come to find three common uses that are present. This section will describe this straightforward social media and Internet use in terms of communication and connectedness, boosting visibility, and promoting and advocating attacks.

To begin with the most basic use of social media for terrorists, one must understand how it is used to promote communication and connectedness. Klausen (2015) explains that the ways illicit organizations use social media to communicate vary. Although some militants consistently update their social media profiles, many are not able to communicate at all. For example, new recruits must turn over their cellphones when arriving at training. So, what may seem as spontaneous communications uses, are actually calculated and controlled (Klausen, 2015, p. 2). A commonly held threat of the Islamic state is the ability to now communicate globally with potential sympathizers and recruits. A clear example illustrating connectedness and communication is the twitter page “@shamiwitness” which Chatfield et. al., (2015) analyze. They collected and examined 3,039 tweets from this known information disseminator for the Islamic State cause. The results reveal “Shamiwitness” mentioning 877 users, which creates dynamic social networks. Their findings produce evidence of the presence of distinct twitter populations, which include international media, regional media, actual Islamic fighters, and Islamic State sympathizers. These networks transcend international borders and directly ask users to join their cause (Chatfield, et al., 2015, pp. 4–11). Richards (2014) points out that in 2014 ISIS had 9,000 foreign fighters and around 3,000 were western recruits and attributes this phenomenon to the use of social media to communicate across borders. In her article, she mentions a study on social media of foreign fighters, which expose the direct influence of Australian ISIS supporters. Only 35 twitter accounts create a network of 18,223 specific users. These online accounts created by terrorists and their organizations are able to reach an unprecedented about of users. In Michael Steinbach's (2016) Statement before the Senate Committee on Homeland Security and Governmental Affairs, he explains the dangers of evolving communications by giving the example of an unnamed individual apprehended for providing aid in facilitating an associate's travel to Syria to join ISIS. He revealed that the individual had several connections through social media with "like minded individuals". The fact that terrorist organizations' means of communications have improved is undeniable, what must be examined next is how they utilize this communication and connectedness to boost the visibility of their messages and propaganda.

Terrorist organizations not only deploy social media networks effectively to communicate and connect with others, but to boost the visibility of their messages and propaganda. They have seized the opportunity to spread their messages to a wider range of communities with similar ideologies as theirs. Propaganda throughout history has been essential to terrorism. The idea of propaganda by deed is intensified and altered through these Internet platforms. This is the idea that acts of violence will serve as a catalyst to political change and revolutionary movements. In order for this process to be effective, they must reach the greatest audience possible. To begin with, terror organizations will magnify external threats from outsiders and the government. They then attack their governments which in turn elicits a sometimes-violent response (Chatfield et. Al., 2015, p). Taking Nizar Trabelsi as an example of this, he claimed that he made the decision to carry out an attack as an associate of Al Qaeda after seeing pictures of a killed Palestinian baby on the Gaza Strip (Archetti, 2015, p. 55)[3]. Many saw this picture, but after it spread, it reached a person willing to kill for a terrorist organization. Klausen (2015) elaborates on the ISIL (ISIS) offensive

[3] Nizar Trabelsi was once a pro football player from Tunisia who conspired with Al Qaeda, specifically Osama bin Laden, to carry out a suicide attack targeting Americans in Europe. He was arrested in Belgium before he could complete his attack. To read more about Nizar Trabelsi please visit https://archives.fbi.gov/archives/washingtondc/press-releases/2013/alleged-al-qaeda-member-extradited-to-u.s.-to-face-charges-in-terrorism-conspiracy

of 2014, which included graphic photos of beheadings that forced American involvement. These photos are not only meant to incite fear but to illustrate the organizations unconstrained power. Although these gruesome photos are what most hear about, groups like ISIS and Al Qaeda spread photos of their normal day-to-day lives. There are photos of propaganda that show groups of men with guns in hand enjoying a pizza. These clearly staged photos exist to manipulate possible sympathizers into believing that life as a jihadist can be rewarding and even normal (pp. 12–13). Organizations take the message they want and can spread them on a multiplicity of social media pages creating the redundancy necessary to ensure their propaganda reaches wide audiences. A few may not see the immediate threat in spreading propaganda, but the threat is undeniable when calls advocating for and praising individual attacks begin to appear.

An immediate threat that the use of social media networks by terrorist organizations poses is the call to arms. Many go beyond trying to persuade sympathizers to join their fight, but rather to take the fight into their own hands, wherever they might be. They have the direct ability to inspire what some call "lone wolf attacks" around the globe all from behind a computer screen or just a smartphone. Looking at the attack in San Bernardina in 2015 and in Orlando in 2016, we see the Islamic State does have the ability to inspire some sort of attacks without any direct contact or control over the attackers. According to Daniel Byman (2017), both attackers claimed allegiance to the Islamic State but were not directly controlled or involved with a terrorist group. These so-called "Lone Wolves" managed to kill 63 Americans (Byman, 2017)[4]. Terrorist organizations can be more specific with their goals for lone attackers. For example, United States Military personnel were targeted when a list of hundreds of names of serving members was released and spread through social media by terrorist affiliated networks (Steinback, 2016). The ability to attack around the globe outside of specific illicit organizations is only growing as social media grows.

This section explains in simple terms how terrorists and their illicit organizations utilize social media and the Internet. After reviewing several of the cited sources which include news article, studies, and research three common

[4] Daniel Byman explains in his article "Beyond Iraq and Syria: ISIS' Ability to conduct attacks abroad" that although the two examples of "Lone Wolf" attacks mentioned in this article claim some affiliation to the Islamic State and ISIS claimed ownership of the attack, there are several other potential factors that contributed to their attacks that have nothing to do with terrorism at all. To read further about this go to https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/

uses of the Internet by terrorists that are relevant to this paper were picked out. The use is outlined in terms of communication and connectedness, boosting visibility, and promoting and advocating attacks. What must be analyzed next are the actual threats these uses pose.

The Realistic Threat That Terrorist Organizations Use of the Internet is Posing

There appears to be a panic within the media and policymakers concerning the weaponization of the Internet and social media sites to aid terrorist efforts. The threat cannot be completely dismissed because access to the Internet does raise the efficiency of the tactics the terrorist organizations employ. Unfortunately, many think that with the use of the Internet, terrorist organizations could radicalize people into terrorists around the globe. This causes an unnecessary demonization of the Internet and social media sites. In turn, many lose focus of the larger picture of recruitment, which includes a social aspect that exists beyond the Internet. This section elaborates on two facets that need to be taken under consideration when assessing threat levels. First, terror organizations deploy similar tactics that they have been using throughout history, but it is just now applied to the Internet. Next, that the Internet alone is not enough to radicalize and recruit an individual.

There are traditional tactics that terrorist organizations employ which seem to be sparking a panic due to the use of the Internet. For example, a common tactic to recruit to organizations is to target the Islamic youth, specifically males that may be looking for a place to fit in. They proceed to recruit by attempting to strengthen their identification within a group (Chatfield et. al., 2015). This is now accomplished online in various steps which are explained by JM Berger (2015) as discovering a vulnerable recruitment target, creating a micro-community around him or her, isolating them from friends and family, privately communicating with them, then finding out what actions the recruit would be willing to do and encouraging them. The only difference is that now this is being applied through social media sites like Facebook, Twitter, and YouTube. Although these sites are helpful tools in the process of radicalization, they alone are not enough to complete the process.

Social media networks make the radicalization process for organizations more efficient, but Archetti (2015) explains that radicalization and extremism happen in a social sphere that is constituted by several overlapping networks.

Individual narratives compose these networks. By narrative, Archetti means that each individual person has his or her own mentality at any moment in time. Any information that an individual receives from terrorist organizations is taken into and interpreted through their own narrative at that moment in time. A person's relationships and narratives are consistently changing. Whether a person is receptive to recruitment tactics is dependent upon the connection with that potential recruit's narrative and a member of/or the group's narrative. These social media platforms are a tool but the operators, networks, and the tactics they implement are central to radicalization. To simplify this idea, the Internet cannot radicalize without a preexisting narrative that is open to the idea of extremism. Looking at the example of Nizar Trabelis again, who attempted an attack after seeing a picture of a killed child on the Gaza Strip, thousands saw the picture of the child but only he was persuaded to organize an attack. Archetti (2015) stresses that this occurred because he was the one individual who already possessed a narrative receptive to radicalization (Archetti, 2015, pp. 53–54). What the Internet is able to do is spread a message wide enough to reach an individual with the potential to be radicalized, and that threat cannot be fully dismissed.

Part of what makes Jihadist organizations use of social media platforms successful is volume. With the creation of these platforms, organizations can mobilize supporters and fundraise in more efficient ways. They can reach a broad audience with a greater opportunity to connect with sympathizers. Doing most of this online, they are often working anonymously. All these things are reasons that many consider the Internet to be a modern weapon for terrorism. The existence of these threats is not something to be disputed. What can be stated is that the reaction to these developments is disproportionate. Two important factors are explained that touch on the idea that the main factors pertaining to radicalization and recruitment are not the Internet at all but rather their use of traditional tactics, and importance of individual and group narratives. Since many do not argue the existence of a threat, one should consider potential counter efforts to keep up with rapidly advancing technology.

What We Can Do

It is not enough to discuss how terrorists utilize the Internet and social media in their recruitment tactics and the threat levels surrounding this activity. Arguably the most important portion of this paper is outlining potential efforts to minimize and counter the damage done by terrorist organizations online.

These ways include evolving law enforcement tactics, taking a community-based approach, and finally holding our media and news networks accountable.

To begin with, the most obvious defense to any terrorist activity is law enforcement. Michael Steinbach (2016) explains how pertinent it is for all law enforcement to be familiarized and be able to monitor the latest communication tools that terrorist organizations utilize. Steinbach does highlight some challenges that accompany this task. The forms of communication in the information age are outpacing the ability of our government agencies to keep track of them. Normally, law enforcement agencies have the ability to access stored communications with a lawful process but there are services developing that do not store any information at all. The lack of familiarity with new communication technologies is what Steinbach refers to as "going dark." JM Berger (2015) suggests a consistent analysis of social media, which can detect communities affiliated to Jihadist groups. Following confirmed recruiter profiles, law enforcement can discover potential supporters. At times, the shift from public to private communication can be spotted, and it is at this point that law enforcement must intervene. With the current social media platforms present at this time, there are only so many methods of interaction. Berger states that with the monitoring of social media sites of the recruiter, we can possibly discover the process being commonly implemented. Unfortunately, with evolving technology and its vast span, it would be difficult to monitor every social media account. For that reason, it is important to go beyond the Internet.

Where we may fall short on counter efforts through the Internet, we must make up for with community approaches. There have been attempts to put forth narratives to juxtapose those being circulated by terrorist organizations. This method is ineffective since the narratives constructed by ISIS for example, include all aspects of life. They discuss career opportunities, home life, and attempt to create a sense of community for any potential recruits (Steinbach, 2016). They have an elaborate network to circulate these narratives. Any message sent out by a government agency or organization will fall short. We do not possess the proper networks to receive and circulate any counter messages we may attempt to create. This is where building a community connection becomes essential. Long-term engagement within a community gives the possibility to gain understanding into what Archetti (2015) calls "local narratives" (p. 56). It is also important that this engagement does not consist of solely impersonal communication, but rather through meaningful action. We can become involved through social movements, local charities, and personal communications (Archetti, 2015, p. 56) There is no formula that can discover a potential terrorist, but this is a way to gain trust within societies and begin to recognize why one might be susceptible to terrorist recruitment within a community. This may be a daunting task to accomplish and control but something that is clear is the use of news media outlets.

Some may argue ensuring that news media sources are not making a situation worse is a clear and simple task. In a democratic country with freedom of speech, like the United States, it is almost impossible to control what news media outlets put out. This can aid the efforts of terrorist organizations. As previously discussed, terrorists require large audiences to succeed with their terror tactics. In the past, they would rely on media to spread their messages by continuously reporting and broadcasting them. The way they would force this is by choosing a large symbolic target, like the World Trade Center to attack. Their goal can be explained with a Chinese proverb "Kill one- frighten ten thousand" (Klausen, 2015, p. 2). The current use of social media has changed the dynamic of media reliance. Now that terrorist organizations have their own platform, they choose what to circulate and the media then picks up on it and reports it. They still get the media coverage required to build an audience but now they have more control as to what is being reported and spread. JM Berger (2015) stresses that mainstream media can play a helpful role in not spreading terrorist propaganda and fear by ensuring that the amount of coverage on any incident is proportionate and responsible. Unfortunately, medias disproportionate reporting can be seen with most terrorist attacks in the western world. Media outlets normally lead with the most interesting and often gruesome stories for views, and if there had been a terrorist attack or threat, this will normally lead for a greater period than is appropriate.

Arguably the most important portion of this paper is exploring potential solutions and counter efforts to combat recruitment tactics. The first means of defense is law enforcement tactics. This cannot provide the most comprehensive countermeasure to recruitment since it is impossible to say with certainty who is susceptible to radicalization online. For that reason, taking a more in-depth community-based approach is stressed. Finally, holding our media and news networks accountable is something we have the potential to do within our own countries. Perhaps more solutions could be discovered and explored but there are limitations to this field of study.

Concluding Thoughts and Limitations

Terrorist organizations use of the Internet and social media is a young field of study. It appears that illicit use of the Internet and social media is developing quicker than our ability to analyze it. Although there are several mass media reports on recruitment through online media sources, there is a lack of academic studies on the topic. Not only is there a lack of studies and research on the topic, there also appears to be a lack of consensus on the matter and threat level it possesses. Some contrasting viewpoints have been illustrated in this paper. Another limitation to this field of study is social media policies that both hinder terrorist's capabilities to communicate but also researcher's abilities to research. Chatfield et. Al., (2015) explain when analyzing the "@shamiwitness" twitter account that social media sites like Twitter and Facebook have a policy in place to suspend or terminate any account associated with a terrorist organization. These accounts are disappearing and reappearing with similar but different names to go undetected, making it difficult to track their activity.