Fighting Extremism: Efforts to Defeat Online ISIS Recruitment Methods

Michael Howell
University of Mississippi. Sally McDonnell Barksdale Honors College

Follow this and additional works at: https://egrove.olemiss.edu/hon_thesis
Part of the Defense and Security Studies Commons

Recommended Citation

This Undergraduate Thesis is brought to you for free and open access by the Honors College (Sally McDonnell Barksdale Honors College) at eGrove. It has been accepted for inclusion in Honors Theses by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.
Dedication

I dedicate this thesis to my parents, Paul and Wanda Howell, who supported me in every way throughout my undergraduate journey. Not only did they encourage me to always do my best, but they also challenged me to strive for new challenges and push my limits in order to become a better version of myself. For that, I am forever grateful.
Acknowledgements

This project would not have been possible without the tireless efforts of my thesis advisor, Dr. David Bath. Over the course of the last year, Dr. Bath went beyond what was expected of him to help me improve as a student, citizen, and human being. My appreciation for his heart and intellect will only continue to grow.

I would also like to thank my readers, Dr. David Rutherford and Dr. Vivian Ibrahim, for utilizing their talents to assist me in enhancing my thesis; the Sally McDonnell Barksdale Honors College for affording me outstanding opportunities to develop into a citizen scholar; the Trent Lott Leadership Institute for advancing my leadership skills and understanding of public policy; the Center for Intelligence and Security Studies for shaping the passion, abilities, and network I will need in order to fight terrorism; and The University of Mississippi for the best years of my life so far.
Abstract

The Islamic State of Iraq and Syria (ISIS) and its sympathizers utilize social media platforms to disseminate propaganda, radicalize audiences, and recruit foreign fighters. Some Western social media users are susceptible to these efforts. Although personal privacy and freedom of speech is largely protected by complex governmental limitations, the social media use of extremists sparked a national debate on how to protect American citizens. This thesis will discuss the history of ISIS and its social media use, the terrorist group’s target audiences, ISIS recruitment strategies, and policy decisions and options aimed at reducing the effectiveness of pro-jihadist propaganda. This paper will explain what the United States can implement, already implemented, and could implement in the future.

*Keywords: ISIS, jihadist, social media, policy*
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>i</td>
</tr>
<tr>
<td>Copyright</td>
<td>ii</td>
</tr>
<tr>
<td>Dedication</td>
<td>iii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>iv</td>
</tr>
<tr>
<td>Abstract</td>
<td>v</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>vi</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Chapter 1: History of the Formation of the Islamic State</td>
<td>3</td>
</tr>
<tr>
<td>Chapter 2: History of Online ISIS Propaganda, Radicalization, and Recruitment</td>
<td>8</td>
</tr>
<tr>
<td>Chapter 3: Seeking a Target Audience</td>
<td>13</td>
</tr>
<tr>
<td>Chapter 4: Radicalization and Recruitment Tactics</td>
<td>18</td>
</tr>
<tr>
<td>Chapter 5: Counterterrorism Efforts</td>
<td>30</td>
</tr>
<tr>
<td>Chapter 6: Conclusion</td>
<td>57</td>
</tr>
<tr>
<td>Works Cited</td>
<td>59</td>
</tr>
</tbody>
</table>
Introduction

The Islamic State of Iraq and Syria (ISIS) radicalizes and recruits Americans through social media and will likely continue its successful social media campaign over the course of the next year since the Shiite governments in Iraq and Syria remain in power. In order to comprehend the success of ISIS, one would benefit from understanding how the organization formed, the evolution of its social media presence, the target audience of the ISIS social media campaign, and the tactics utilized by ISIS recruiters after Westerners have been radicalized.

Throughout this thesis, the term “radicalization” is within the context of Islamic extremism. Within this context, the author of this thesis utilizes the definition of radicalization from the New York Police Department report “Radicalization in the West: The Homegrown Threat.” The article defines radicalization as “the progression of searching, finding, adopting, nurturing, and developing this extreme belief system to the point where it acts as a catalyst for a terrorist act” (Silber and Bhatt, 2007, p. 16). Since radicalization can be described as a spectrum of progression, some individuals are more radicalized than others. For that reason, some people may simply hold radical beliefs while others act on said beliefs.

In order to describe current radicalization issues and public and private policy decisions to confront terrorism, this thesis utilizes news outlet sources since academic sources are often not as current. The author of this thesis utilized academic sources, however, when researching information that did not change throughout the course of researching for this thesis, such as the history of Islam and the Islamic State and the target audience of the ISIS recruiters.
This thesis examines the creation and goals of ISIS and its use of social media to recruit followers. It also explores the public and private sector methods to combat such efforts. Chapter 1 explains how a faction of al Qaeda evolved into a separate terrorist group known as ISIS. In addition, it briefly describes the history of Islam and why ISIS has gathered so many Sunni followers. Chapter 2 details how and why ISIS and other terrorist groups began utilizing social media for radicalization and recruitment rather than other forms of communication. It also explains how ISIS uses social media to disseminate propaganda to wide audiences throughout the world. Chapter 3 details which people, based on current information, are most susceptible to ISIS recruitment efforts. In Chapter 4, the study illustrates the detailed process ISIS recruiters use to radicalize people through contact on social media. Additionally, the chapter describes the different approaches ISIS uses from an al Qaeda recruitment manual to radicalize people of various backgrounds and beliefs. Chapter 5 describes and analyzes numerous counterterrorism efforts, both successful and unsuccessful, implemented by the public and private sector. The public sector conducts counterterrorism projects, sting operations, and military strikes on ISIS targets. Private sector companies remove ISIS-sympathetic profiles that break terms of use agreements, reroute potential recruits to anti-jihadist propaganda, and report legitimate threats to law enforcement officials, among other practices. Finally, Chapter 6 consists of recommendations to improve current counterterrorism efforts so that they will be more successful in the future. This chapter also argues the overall success of the counterterrorism policies implemented by private and public American groups since the creation of ISIS.
Chapter 1: History of the Formation of the Islamic State

When the United States government overthrew Saddam Hussein in 2003, the power vacuum allowed many terrorist groups to organize and take control. Many terrorist organizations originally held political goals, but they began to gain support by shifting their focus to religious tribalism. Much of the rise of ISIS stemmed from unrest between Shiite governments and largely Sunni citizen populations. ISIS heavily focused on the divisions between the Islamic sects in order to gain support from angry Sunnis. For that reason, it is important to understand the two sects of Islam (Celso, 2015).

Sunnis and Shiites represent two major sects of Islam, and the schism between the sects can be traced back to the succession of leadership in Islam after Muhammad. Muhammad’s son-in-law, Ali, became the leader of Islam after his father-in-law’s death. The term “Shi’at Ali,” which evolved into the word “Shiite,” means the “partisans of Ali.” Originally, Muhammad’s followers did not allow Ali to succeed the leadership position, but the Shi’at Ali argued that Muhammad named Ali and his family the leaders of Islam. Eventually, Muhammad’s disciples agreed, and Ali became the Islamic leader who later passed his leadership to his son Hussein. Shiites believe that the teachings of Muhammad and twelve caliphs, comprised of some of Muhammad’s direct descendants including Ali and Hussein, are the true authority of Islam. In the Shiite belief, only those thirteen men are considered the mediators between God and the world (“The Unending Feud,” 1987).

On the other hand, Sunnis honor Ali, but they do not consider him or the other eleven caliphs as people who directly interacted with Allah in ways that other Muslims cannot. Instead, Sunnis believe that anyone can have a direct relationship with Allah if
the person follows the Quran. The word “sunna,” which is the root of the word “Sunni,” means “the tradition of the Prophet,” which places emphasis on tradition rather than heredity. Conflict has taken place between the two factions for generations. In fact, “in the eyes of the Shi’ites, any regime not under the rule of the Prophet’s true heirs is an abomination” (“The Unending Feud,” 1987). Shi’ite governments continue to hold this stance, which continues strife in the Middle East such as the Sunni rebellions against the Shiite Iraqi and Syrian forces.

By 2013, al Qaeda in Iraq (AQI) became ISIS, which operates mainly in Iraq and Syria. AQI took advantage of the power vacuum left by the withdrawal of United States military troops in Iraq to increase its power in the country against the Shiite prime minister, Iraqi Prime Minister Nuri al-Maliki. Many Middle Eastern Sunnis believe that Al-Maliki repressed Sunni political opponents, and many local and foreign fighters joined AQI in battle against the Shiite government of Iraq. Numerous fighters who battled in Iraq later fought against the Shiite government of Syria in the Syrian civil war as well since both governments allegedly mistreated Sunnis (Celso, 2015).

AQI utilized social media to recruit Sunnis from around the Middle East to join in the fight against the Shiite governments of both Iraq and Syria. Recruitment efforts, both online and offline, were so successful that more than ten thousand Sunni Muslims from other countries (hereafter referred to as foreign Sunni fighters) joined the Syrian civil war by the end of 2013 while thousands also fought in Iraq. Due to the resurgence of Sunni power in the region, Abu Bakr al-Baghdadi, the leader of AQI, decided to rename his faction of al Qaeda the “Islamic State of Iraq and Syria” (ISIS) in April 2013. Although
the group was still a part of al Qaeda, al-Baghdadi believed that ISIS deserved individual notoriety (Celso, 2015).

The name “Abu Bakr” resonates well with many Muslims since the first caliph after Muhammad’s death was a man named Abu Bakr. Bakr was Muhammad’s father-in-law and the first Muslim that was not a blood relative of Muhammad (“Abu Bakr”). Abu Bakr al-Baghdadi’s name could produce thoughts of the highly praised Muslim figure, similarly to how Pope John XXIII had a name that reminded Christians of the apostle John.

Abu Bakr al-Baghdadi followed in the footsteps of his Sunni predecessor in al Qaeda leadership, a man named Abu Musab al-Zarqawi, who was killed by an American drone strike. During his time as an al Qaeda leader, al-Zarqawi declared that he envisioned an eventual Sunni caliphate that was free of opposing religions and cultures. Fellow al Qaeda members criticized both al-Zarqawi and his follower al-Baghdadi for their unrealistic ideology of a Sunni caliphate. In February 2014, al Qaeda’s leadership expelled ISIS from the rest of the terrorist group, which gave al-Baghdadi the freedom to alter the goals of ISIS (Celso, 2015).

Several developments allowed al-Baghdadi to make al-Zarqawi’s dream a reality: a weakened Iraqi government following the overthrow of dictator Saddam Hussein, the ISIS success in Syria, and the Islamic State’s division from the rest of al Qaeda. Eventually, ISIS controlled large swaths of land near the Iraqi-Syrian border due to the size and force of the organization. In June 2014, al-Baghdadi issued a statement that ISIS had become an independent Sunni caliphate. The caliphate grew throughout 2014 as ISIS took control of more land throughout the Middle East (Celso, 2015).
ISIS members’ faith in the guidance of al-Baghdadi as an official caliph led to much of the success and growth of the jihadist group. Al-Baghdadi’s followers often refer to him as Caliph Ibrahim, since Ibrahim is his birth name and the word “caliph” means “successor” to the Prophet Muhammad (Wood, 2016, p. 16). According to Muslim tradition, four “rightly guided caliphs” led Muslims after Muhammad died in 632 until 661 (Wood, 2016, p. 15). Since a true caliph is a successor of Muhammad, a caliph can demand devotion from all Muslims, as al-Baghdadi does. A caliph, historically, must adhere to specific requirements. In order to be a caliph, a person must be male, a devout Muslim, adult, free of physical and mental handicaps of any kind, and come from the Quraysh tribe in the Arabian Peninsula. The original “rightly guided caliphs” supposedly held each requirement, and al-Baghdadi says that he fulfills each requirement as well (Wood, 2016, p.16).

Over the past few centuries, many declared caliphates have been lax on the requirements for caliphs. Historically, many of the so-called caliphs were unsuccessful leaders. Some Muslims believe the leaders did not meet the requirements to actually be caliphs, which is why they were unsuccessful (Wood, 2016, p. 16). Well educated Islamic scholars from Iraq and Syria who have pledged their allegiance to ISIS argue that al-Baghdadi is the eighth legitimate caliph in history, since he and the other caliphs recognized met all the necessary criteria. One of the ISIS Islamic scholars, a cleric named Turki al-Bin’ali, declared that Muhammad guaranteed that there will only be twelve caliphs before the end of the world. A Rice University history professor named David Cook noted that, according to literal interpretations of certain Quranic texts and quotes from certain imams, “the battles preceding the Day of Judgment will take place in
modern Syria, with a final showdown in the year 1500 of the Islamic Hijra calendar, or A.D. 2076” (Wood, 2016, p. 17). Many of al-Baghdadi’s followers believe that Caliph Ibrahim is continuing the prophesy of the Quran, and they are destined to continue his goals no matter what opposition they face. Al-Baghdadi’s favorability and notoriety as an official caliph coupled with ISIS success against Shiites gave the terrorist organization an appearance of legitimacy. In order to spread the message of the caliphate, expand the group’s ideological support throughout the world, and accumulate more members, the group utilizes social media (Celso, 2015).
Chapter 2: History of Online ISIS Propaganda, Radicalization, and Recruitment

The ISIS caliphate utilizes the internet, specifically social media, to gain support through political propaganda, radicalization, and recruitment. After some viewers observe political propaganda from the Islamic State, they believe that the group’s ideology is worthy of believing and that the terrorists are actually fighters for good. Once someone believes ISIS propaganda, he or she is then radicalized whether or not the person actually acts upon those radicalized beliefs. After a person is radicalized, he or she may contact a radical social media user or be contacted by ISIS members or sympathizers who will attempt to convince the person to join the terrorist organization. This process became simpler and more successful than it was in the past due to access to the internet (Chatfield et al., 2015).

Terrorist networks have utilized numerous forms of media throughout history, but the media could be expensive, difficult to disseminate to large audiences, and not as successful as the internet is. In the past, for example, some terrorist organizations employed fliers to inform potential recruits about the groups’ goals, ideologies, and other important information. Compared to the internet, the fliers were expensive, more difficult to broadly share with large numbers of local people, and not very effective in the recruitment of Westerners from overseas (Chatfield et al., 2015).

ISIS also benefits from another positive aspect of the internet: people can view web pages and emails at any time from numerous locations and on multiple devices like computers and smartphones. The internet revolutionized the dissemination of terrorist propaganda, and ISIS members and sympathizers can use social media wherever they have internet connection. Additionally, because terrorists are now able to utilize
anonymous chartrooms and social media accounts to attempt to radicalize and recruit people, they can reduce the risk of prosecution. Ease of access and anonymity to this degree are benefits that were widely unavailable to terrorist recruiters before they utilized social media platforms (Chatfield et al., 2015).

The following example demonstrates how powerful even one ISIS sympathizer’s social media account can be when it comes to reaching others. From February 2013 to February 2014 a research team examined 2,405 Twitter accounts that foreign fighters read on a regular basis. Out of all the accounts examined, 1,778 users, or approximately 74 percent, had only one jihadist follower each. Only 46 users, or approximately 1.9 percent, had 10 or more jihadist followers each. However, one Twitter account, with the username @shamiwitness, was “the most popular and influential Twitter user to the foreign fighters in Syria” (Chatfield et al., 2015, p. 241). The account had approximately 17,700 followers (Raidió Teilifís Éireann, 2014) and made thousands of posts in English in order to reach a Western audience. Although @shamiwitness had no official connections to any jihadist organizations, it politically and morally supported jihadists in Syria. Unfortunately for the researchers, however, it is impossible to determine exactly how much impact the account had on its audience since radicalization does not always result in action. An American may accept ISIS ideology, for example, but never carry out attacks or fight overseas for the organization. Despite the above limitation, however, the researchers were able to view how well the account assisted individual jihadists by sharing their information to a larger audience (Chatfield et al., 2015).

Twitter shut down all of the most popular jihadist accounts examined in the research by October 6, 2014, except for @shamiwitness. Over the course of October
2014, the account sent thousands of tweets from its account. Although an official member of ISIS did not run the account, the far-reaching dissemination of information led Indian authorities to believe that the account was too dangerous for the government to not arrest its user. After the arrest of the @shamiwitness operator on December 13, 2014 in India, Twitter also removed his account like the other jihadist accounts. ISIS received free advertisement, and some Twitter users may have become radicalized, due to @shamiwitness, and that required no extra work by the terror organization. The user’s dedication to the group and his dissemination of information shows how much of an impact a single person can have if he or she becomes radicalized by ISIS (Chatfield et al., 2015).

Some of the most useful tools to help disseminate information, which @shamiwitness utilized, are sharing, replying, and “hashtagging.” Sharing a post on social media, or “retweeting” on Twitter, takes information posted by a certain account and shares it through another account. Anyone who shares a post on his social media page enables all of his followers to see the shared post. If hundreds or thousands of accounts share a post, hundreds or thousands of other people could see it, if not more. Each time @shamiwitness retweeted a radical account on Twitter, all of his followers could witness the post and retweet it to their followers. Whenever a person replies or comments on a post, his followers are often able to see the response as well as the original post, whether they follow the account that created the original post or not. If @shamiwitness responded to a radical Twitter user, people who were not originally following that radical would be exposed to a new jihadist account to follow (Chatfield et al., 2015).
One of the reasons @shamiwitnes was so successful in attracting a large audience was because the user constantly tweeted or retweeted about subjects related to jihad. Another reason was that it retweeted numerous sources that likely added to the user’s credibility. Gathering thousands of followers can be difficult for a social media account. If successful in gathering such numbers, however, an account can widely disseminate information to various countries and various types of people (Chatfield et al., 2015).

The @shamiwitnes account utilized specific hashtags in order for its followers to see what the user, and other users similar to @shamiwitnes, said about a certain subject or belief. “Hashtag” refers to a way in which people around the world can see posts about a particular topic. A “hashtag” is a word or phrase preceded by the “#” symbol. Although the tool began on Twitter, it is also widely utilized on social media sites such as Facebook and Instagram. For example, if someone wanted to see what people around the world are saying about Syria, he could simply search “#Syria.” Disseminating information, therefore, can be quite effective on social media, and it has the potential of reaching large swaths of people if users attract large audiences (Chatfield et al., 2015).

Many ISIS and ISIS-related Twitter accounts organize hashtag campaigns. They pick a specific hashtag, such as #CalamityWillBefallUS in 2014, and encourage their supporters to post numerous tweets that incorporate the hashtag. The more times a specific hashtag is posted on Twitter, the more likely it is to trend. All Twitter users can see a trending list of the most popular hashtags on the website. ISIS members hope their hashtags will surface on the trending list in order for their message to reach an even larger audience (“Hashtag Terror,” 2014).
ISIS has yet to successfully make a hashtag trend since other popular topics usually receive more attention. For that reason, ISIS encourages utilizing hashtags that are already trending. For instance, if ISIS accounts use the hashtag #2016election on Twitter, people who search that hashtag may inadvertently read tweets filled with ISIS propaganda that are among discussions covering presidential election news (“Hashtag Terror,” 2014).

In order to best disseminate information, ISIS mainly utilizes Twitter. Besides the anonymity and dissemination capabilities of Twitter described previously, the organization depends on the social media website for account replacement. After anonymous accounts began sharing the ISIS propaganda video of the execution of American journalist James Foley in 2014, Twitter adopted a more stringent security policy that allowed the company to remove ISIS-related accounts that shared imagery from the video (“Hashtag Terror,” 2014). Once Twitter deletes or suspends accounts, however, ISIS members and sympathizers can quickly create new accounts to continue sharing propaganda. Although ISIS members and sympathizers utilize jihadist Facebook pages, for example, the pages are much more difficult to manage than Twitter accounts. Facebook pages often take longer to create, and the security policies often restrict more jihadist content. Subsequently, Facebook deletes more accounts than Twitter (“Hashtag Terror,” 2014).
Chapter 3: Seeking a Target Audience

ISIS utilizes social media to successfully radicalize people and disseminate information, but recruitment usually occurs through other means. Despite the common assumption that online recruiting is extremely successful throughout the West, one German study determined that only about 18 percent of German jihadists have been recruited over the internet. Despite the fact that a majority of recruitment does not occur from social media and other websites, ISIS recruiters still gain nearly one fifth of their recruits from online sources. That is a substantial number of recruits that can become interested in ISIS from other countries with little to no immediate personal interaction with the organization (Franz, 2015, p. 10).

The two strongest methods of recruitment in Germany are communication with radical mosques and imams (23 percent of recruitment to radical organizations) and communication with loved ones who have fought in the name of jihad (30 percent of recruitment to radical organizations). Communication, in this sense, usually referred to discussions in person, over the telephone, or through some other form of one-on-one conversations. It is important to note that although social media accounts “often initiate interest in the jihad, recruitment is a more complex issue and does usually not occur via electronic means” (Franz, 2015, p. 10).

In order to recruit interested people on social media that may not be able to be easily contacted in person, ISIS rewarded members for their online efforts. According to Elzbieta Karska, a Polish human rights lawyer who chairs a United Nations committee that is studying ISIS recruitment, recruiters received from 2,000 dollars to 10,000 dollars per recruit in 2015 depending on the quality of the person (Winsor, 2015). ISIS was able
to pay their recruiters large amounts of money because the organization had control over numerous oil fields in the Middle East that provided funding to the caliphate, and they also tax people who live within the caliphate (Masi, September 8, 2014). Karska stated, “If [recruits were] well educated like computer specialists or doctors, [recruiters] were paid more” (Winsor, 2015). Additionally, recruiters received a monetary bonus if two of their recruits marry because they may produce children who will become future members of the caliphate. Social media allowed ISIS members to seek more well educated people from the West, which resulted in higher pay (Winsor, 2015).

Recruiters approach Westerners in different ways according to the potential recruits’ beliefs or social status. In a 2015 *Mediterranean Quarterly* article entitled “Popijihadism: Why Young European Muslims Are Joining the Islamic State,” author Barbara Franz, a political science professor at Rider University, recorded findings from her research on the demographics of ISIS recruits. Franz assessed that “most Western fighters are men under forty years of age” (Franz, 2015, p. 8). Franz argued that the reasons Western Muslims are specifically attracted to ISIS vary widely, but three reasons are common: the rise of a Sunni caliphate that could one day rule the world, the fight against oppressive Shiite governments in Syria and Iraq, and an escape from Western communities where many Muslims do not feel welcome (Franz, 2015, p. 8).

First, many ISIS recruits wish to join the terrorist organization because of the idea of a pure and unified caliphate. Many young fighters see the caliphate as the future of Sunni Islam, and they think that it is only the beginning of a regime that will eventually spread across the world. When ISIS fighters began to kill Kurds, Christians, and other people groups, the terrorist group posted the videos of the killings on social media. Franz
stated, “Once IS began to attack Kurds and slaughter Yazidis instead of [President] Bashar al-Assad’s soldiers, the logic surrounding the jihad as a holy war against unbelievers became the key justification for jihadism” (Franz, 2015, p. 8). For many, seeing people of different beliefs as infidels made it seem as if ISIS was on the offensive for the sake of religious purity rather than for the sake of political gain. Viewing ISIS violence as grounds for religious cleansing rather than simple fighting between different political groups attracted numerous Westerners to the cause of ISIS, and many even traveled to the Middle East to join the fight against people who they believed to be infidels (Franz, 2015).

The second reason that some Western Muslims, specifically those in Europe, joined ISIS was to fight against Syria and Iraq. More Western Muslims fought against Syria than Iraq because they considered President al-Assad’s government responsible for the two hundred thousand dead civilians and millions of displaced Syrians, which many fighters saw as genocide. ISIS members and sympathizers in the region largely accepted that the Shiite government incessantly killed civilians simply due to their Sunni faith. Numerous Westerners wish to fight alongside ISIS because they consider themselves heroic rescuers who are completing the will of God, as declared by numerous ISIS videos and speeches. The desire to become a hero to a nation while simultaneously desiring to experience adventure is referred to as the “Hemingway Phenomenon,” (Franz, 2015, p. 8) named after Ernest Hemingway who fought in the Spanish Civil War in a desire for justice and adventure. Soldiers throughout history, despite the war or situation, often feel allegiance to those with whom they fight side-by-side. That bond, along with the “Hemingway Phenomenon,” caused Westerners to be even further radicalized into other
acts of jihad around the world. When there is trust and mutual respect between two
soldiers who have protected each other, it is more likely that one would sympathize with
the other’s beliefs about a wide range of topics, including jihad. Once someone becomes
radicalized by one of his or her fellow fighters, that person could then be utilized as a
social media recruiter, or another type of ISIS recruiter, in that person’s Western country
(Franz, 2015, p. 9).

For some Muslims who immigrate into the West, or even first generation Western
Muslims, the main cause for radicalization is not the caliphate or the desire to become a
hero. Instead, the third reason that some Western Muslims are radicalized due to issues
with integrating into the West and finding social mobility. Issues that plague these
Muslims, such as alleged racism and loneliness due to being an outsider, often lead to
psychological issues. Additionally, most of the jihadists examined in the study who held
jobs worked for minimum wage in a low-skill occupation. A recent study of German
radicals found that 249 of the 322 who went to fight with ISIS had committed a crime in
the West. Many of these crimes were violent and included drug offenses and theft. “Jihad
attracts people who feel they do not have a legal and social space within the German and
European society” (Franz, 2015, p. 19). Western Muslim immigrants, who sometimes
experience racial and religious discrimination, are able to witness mosques in their new
countries that offer an apparent unity that they do not often experience in other places
within the Western world. Some radical Western mosques, for example, consist of people
of many nationalities and ethnicities praying next to each other and interacting together.
The uniting of different races and nationalities through the ISIS ideology can entice
Westerners who may feel like outsiders in their new countries. Therefore, Western
Muslims who accept this idea of unity often do not recognize that the inclusivity does not include different interpretations of Islam (Franz, 2015, p. 11).

Although the above reasons explain why some Sunni Muslims in the West join ISIS, it is important to acknowledge that a common misconception about Westerners who become radicalized by ISIS is that they are all poor and/or Muslim. A 2016 article entitled “Vulnerabilities among young Westerners joining ISIS” contends that a majority of Western ISIS fighters are financially stable, and many were not originally of the Muslim faith. Similarly to Franz’s assessment, however, the authors concluded that much of the ISIS appeal stems from the organization’s ability to provide an identity to people who do not currently have confidence in their own. According to the report, the majority of people radicalized by ISIS are “everyday young people who are in social transition, on the margins of society, or amidst a crisis of identity” (Yu and Haque, 2016). All three issues are related to the difficulty of finding an identity as young people transition into adulthood. Joining ISIS helps discouraged youths feel a true sense of purpose and identity.

Dr. Seong Yu and Dr. Sultan Haque, who wrote the report, argued that psychological studies have shown that humans tend to seek certainty when developing beliefs. Ideologies or beliefs that leave ambiguities or uncertainties are often unattractive to individuals compared to beliefs in absolute certainties. The worldview of ISIS leaves no room for ambiguities, and it splits the world into absolute good and absolute evil. Radicals sometimes easily accept rigid and simplistic beliefs because they desire structure in a liberal Western society where they do not feel accepted (Yu and Haque, 2016).
Chapter 4: Radicalization and Recruitment Tactics

ISIS utilizes differing strategies when disseminating propaganda. When appealing to locals, ISIS often generates solidarity within the Sunni Muslim community, emotionally connecting with local issues, providing religious reasons to fight infidels, and promoting the organization’s ideologies. In Syria, for example, ISIS recruited Sunnis by letting them know that ISIS came to protect them and provide them with reinforcements to fight the Shiite government (Chatfield et al., 2015).

But when appealing to the global community of both Muslims and others, the group tends to show that ISIS is feared and powerful, intimidating public opinion in the West, arguing the morality of terrorism, and urging people to shift their perspectives on violent ideologies. ISIS seeks to radicalize current Muslims by arguing conservative, Sunni interpretations of Quranic verses. When radicalizing those who are not Muslims, however, ISIS teaches its audience, through videos and readings, why the group believes a radical Sunni faith is supreme. One of the goals of ISIS is to unite Westerners of different backgrounds through the same jihadist views (Chatfield et al., 2015).

ISIS propaganda, including videos and pictures, is usually of extremely high quality and evokes strong emotions in and grasps the attention of potential recruits. Matthew Olsen, director of the National Counterterrorism Center, said, “Importantly, the group… views itself as the now-leader of a global jihadist movement. It turns out timely, high-quality media, and it uses social media to secure a widespread following” (Yan, 2016). Former jihadi and author of “Radical: My Journey out of Islamist Extremism,” Maajid Nawaz, stated, “[Western governments] are way behind. They are far superior and advanced than we are when it comes to new media technologies, social media, when
it comes to video production qualities, and in disseminating their propaganda over the
internet” (Yan, 2016). As stated earlier, ISIS oil and tax money has afforded the
organization the opportunity to buy expensive applications and equipment in order to
produce videos and advertisements that resemble Hollywood quality. Videos include
executions, explosions, music, narrators, and other aspects that showcase the brutality
and power of the group (Yan, 2016).

Max Abrahms, a professor of public policy and political science at Northeastern
University, said that the high quality propaganda videos are not only recruiting
unaffiliated people but also people who are already affiliated with other terrorist groups.
Abrahms said that the brutal videos are partially meant to intimidate rival terrorist groups.
Additionally, the videos help ISIS recruit radicals away from rival groups either out of
fear of defeat or out of the radicals’ desire for power and/or religious purity (Masi,
August 20, 2014).

Official ISIS propaganda comes from its own news organization, the Al Hayat
Media Center. The mission statement of the news center is to “convey the message of the
Islamic State in different languages with the aim of unifying Muslims under one flag”
(Masi, August 20, 2014). In order to convey legitimacy and fear, the news agency
publishes quarterly reports of all attacks and murders committed by ISIS. Additionally,
the agency created a video series called Mujatweets, which ISIS translated into at least
four languages, to convey the caliphate as enjoyable. Displaying both the brutal strength
as well as the alleged “relaxed fun” of the caliphate allows ISIS to appeal to potential
recruits in various ways (Masi, August 20, 2014). Mujatweets often shows ISIS members
engaging in charitable projects, taking care of children, and receiving praise from
civilians. The series also showcases Westerners who joined the caliphate, and they share testimonies about how fun and meaningful their lives became after becoming jihadists (“Hashtag Terror,” 2014).

ISIS also utilizes its online magazine entitled *Dabiq* in order to reach potential recruits and current members. Not only does the magazine include propaganda, but it also includes articles on Quranic stories with radicalized interpretations. Numerous forms of propaganda afford ISIS the ability to reach potential recruits in numerous ways through social media (Masi, August 20, 2014).

One way in which ISIS propaganda often radicalizes Sunni Muslims is by strengthening the idea of tribalism, such as Sunnis versus Shiites, and promoting the idea of defeating the threat posed by the opposing view. The opposing view for ISIS is any group that does not agree with the caliphate’s interpretation of the Quran. An example of the above radicalization strategy would be terrorist networks attacking a Western government or one of its allies simply to evoke a counterterrorism response. The terrorist network is then able to magnify the “political and moral decay” (Chatfield et al., 2015) of the Western government in order to establish a just versus unjust framework that will radicalize certain people.

Additionally, ISIS promotes lone wolf attacks in order to incite fear in and to damage multiple parts of the world at once. Sheikh Abu Muhammad al-Adnani, the official spokesman for ISIS, encouraged lone wolf attacks, in which an individual kills “infidels” in whatever way possible. Al-Adnani says that lone wolves must not fear death. Instead, they must trust that Allah is being glorified through the action. When ISIS members come across an infidel, the spokesman stated, members must “kill him in any
manner or way however it may be. Do not ask for anyone’s advice and do not seek anyone’s verdict” (Chatfield et al., 2015). Al-Adnani’s statement could push individuals to feel self-empowered and religiously obligated to kill others who they believe to be infidels, and many other ISIS members have shared his message. Although no research contends that al-Adnani was directly responsible for radicalizing any of the ISIS-related lone wolves who attacked the Middle East and Western nations over the last two years, the attackers often cite ISIS propaganda as the motive for their jihadist actions (Chatfield et al., 2015).

According to the Institute for Strategic Dialogue, a counter-extremism think tank based in London, more than 3,000 Westerners joined ISIS by 2015 as a result of recruiting on social media and offline. Not all of the Westerners, however, actually traveled to the Middle East to fight alongside ISIS members. Some Westerners simply joined the organization without committing any terrorist acts. Many ISIS magazines and videos attract recruits by making the caliphate seem like a sovereign nation filled with a family of Muslims who simply seek Allah’s will. For men, ISIS claims that it will find them wives and provide them an acceptable place to live and start a family. After ISIS convinces women to move to the caliphate, the women often become “jihadi wives” who will be given over to male recruits (“Three British Schoolgirls,” 2015).

The ISIS approach towards recruiting women is distinctly different than the approach used for men. A social media campaign called “al-Zawra” utilizes posts and videos to explain the role of women in a jihadist setting. The worldwide campaign focuses heavily on domestic activities, such as cooking and sewing, and it explains how important such activities are for the caliphate. Many of the videos also, however, explain
that women will also be utilized for recruitment and combat. In the videos, ISIS members explain that women who join the caliphate will learn technical skills such as software and editing, and they will also learn combat skills, such as hand-to-hand combat and weapon usage. Upon arrival, however, jihadi wives are often also forced into sex slavery for the pleasure of ISIS members (Masi, October 21, 2014).

Another way ISIS utilizes social media to manipulate women is through false narratives. Western and local women have been kidnapped while under the impression that they were coming to certain ISIS-controlled areas for other reasons. Two young women from the United States, for instance, went to Syria believing that they would participate in a humanitarian aid project. Online ISIS recruiters told the women to meet a man once they arrived at the border of Syria, and he would take them to the project location. Once the man helped the women enter the country, he took them to an ISIS compound where he forced them to serve as sex slaves for fighters (Barrow, 2015).

The ISIS treatment of women, even their own recruits, is often abusive. Kidnapped women from the West or other cultures often face more brutality than Sunni women since some ISIS members see them as simply infidels. One of the main reasons women are needed in the caliphate is to bear children who will be the new generation of ISIS fighters (Barrow, 2015).

Members of ISIS manipulate Westerners, such as the example of the American women listed above, in order to recruit them to join the caliphate. As stated by Yu and Haque, lonely young people are sometimes attracted to ISIS due to the ideology giving them another option besides Western society, but they are also attracted to the group because of the attention they receive from recruiters. In order to recruit Westerners,
especially those who are not Muslims, ISIS members utilize an al Qaeda manual from al-Baghdadi’s time in the organization entitled “A Course in the Art of Recruiting.” Unlike Al Qaeda, however, ISIS is very open to who they recruit. Al Qaeda did not recruit women and nonbelievers, since the group sought devout male Muslims, but ISIS recruits everyone that it can since the goal of the caliphate is to continue to grow and gain power (Engel, 2015). The book contains numerous tips and steps that can be utilized in order to recruit Westerners, but one researcher named J.M. Berger at The Brookings Institution summarized the main steps into a simple five-step recruitment process: discovery, create micro-community, isolation, shift to private communications, and identify and encourage action (Berger, November 9, 2015).

The discovery process typically depends on the recruiters. Usually recruiters make connections to potential recruits on social media through mutual friends or family members. Sometimes, however, Westerners attract recruiters due to the potential recruits’ social media activity surrounding ISIS propaganda or jihadist accounts (Winsor, 2015). When Westerners contact or are contacted by recruiters, the potential recruits’ original interest in ISIS can often be traced back to the mainstream media. Western news agencies typically try to be extremely careful in how they cover ISIS news stories so that the reporters do not inadvertently amplify the ideology of the terrorist organization. Despite the agencies’ caution to not advertise ISIS causes, however, the often highly publicize Western recruits, and “many, perhaps most, potential recruits first learn about ISIS from the media, only then seeking it out on social media” (Berger, November 9, 2015).

Some potential recruits may have no faith in Islam before being contacted by recruiters. The ISIS manual actually encourages recruiters to seek nonreligious people
during the discovery process. One passage in the manual states, “You should take precautions against the religious people whom you invite, because maybe they will reject the da’wa (invitation) and end up being the reason for our defeat” (Engel, 2015). As stated previously, ISIS seeks members from groups who are lonely and need meaning in life. The al Qaeda manual suggests that atheists perfectly fit that description. Nonreligious Western youths from Muslim families are preferred due to their non-integration into society, as stated by Franz, and because the manual states that there is righteousness in pointing youth back to their religious Muslim origins. Also, nonreligious Muslims may know many of the basics of the Quran but not a detailed knowledge of Islam. That allows recruiters to likely indoctrinate the youths quicker and easier with their radical interpretation of the text (Engel, 2015).

Spiritual isolation is not the only form of loneliness recruiters seek after for potential recruits, however. The manual calls for recruiters to prey on students specifically, since school can often be a lonely place for vulnerable people. When the book discusses the reason for seeking high school students, it states “the merits of this sector: 1. Often they have pure minds; 2. It is very safe to deal with them because they are not likely to be spies, especially after they pass the stage of individual da’wa” (Engel, 2015).

When discussing college students, the manual places emphasis on the usefulness of both zealousness and loneliness. On this subject, the manual states, “The university is like a place of isolation for a period of four, five, or six years and is full of youths (full of zeal, vigor, and anti-government sentiments)” (Engel, 2015). University students experience a level of independence they never previously experienced. ISIS members use
that freedom and isolation to try to indoctrinate students without being disrupted by others. Once the potential recruits are discovered, a community forms around them (Engel, 2015).

In order to create micro-community, different ISIS recruiters may contact the same Westerner. This makes the potential recruit feel welcome and provides supporting information about ISIS ideology. Recruiters spend thousands of hours developing communication and relationships with potential recruits online, especially lonely people who believe the recruiters to be friends (Barrow, 2015). The manual says recruiters should never go more than a week without speaking to their Western prospects. Also, potential recruits should never be suspicious of the recruiter’s true intent. In the manual, it tells recruiters to “be careful of talking about the problems of the Muslims from the beginning (of the relationship) so as not to make the relationship appear as your recruiting him. He will say to himself, ‘you are doing all of this with me, just to recruit me, etc.’” (Engel, 2015). Instead, the manual assures the reader that he will succeed in recruiting an individual if the process is not rushed. It is at this stage in the process where recruiters may begin speaking about “freedom fighters,” but the manual warns against referring to terrorist groups by name. Additionally, whenever a news program reports on ISIS or similar terrorist groups in a negative way, recruiters are encouraged to argue on behalf of the terrorist groups without specifically endorsing them (Engel, 2015).

Although potential recruits may believe in radical Islam, they may dislike certain terrorist groups because of what they have seen regarding such groups on the news (Berger, November 9, 2015).
For potential recruits of different faiths, ISIS recruiters often urge Westerners to read passages from holy texts that the ISIS members can take out of context. A young Sunday school teacher from Washington who considered herself a Christian, for instance, began to be slowly and unknowingly radicalized by ISIS. People in her new micro-community, after getting to know her, asked her to reexamine certain Bible verses to make sure she actually understood the passages. One recruiter pointed to the verse John 12:44 that says, “And Jesus Christ cried out and said, ‘Whoever believes in me, believes not in me, but in He who sent me’” (Callimachi, 2015). The recruiter explained that although Jesus is a prophet, as accepted in the Muslim faith, he is not actually God. This caused the potential recruit to question her faith and pushed her to trust in the micro-community as well as the Muslim faith in her time of doubt (Callimachi, 2015).

Once they have gained trust, recruiters slowly begin to isolate potential recruits even more from their friends and family. After potential recruits are converted to radical Islam, recruiters often recommend that the new radicals end communication on social media and offline with anyone who may try to influence them to disavow ISIS (Berger, November 9, 2015). In order to avoid suspicion by outside groups and to further isolate radicals, ISIS recruiters often tell potential recruits who convert to Islam to keep their Islamic conversations and faith secret. The recruiters often claim that the secrecy will keep converts from being labeled as terrorists by infidels. Radicals often obey the call to secrecy out of respect to their new companions and out of fear of persecution. Recruiters actually, however, tell recruits to keep Islamic activities secret so that no one will interrupt the recruitment process (Barrow, 2015).
Further isolation can come from recruiters encouraging Islamic studies. As stated in the manual, a recruiter “should also make a schedule for him to listen to at least one lecture daily [by an extremist imam or teacher]. These lectures, books, and pamphlets must become his best friends” (Engel, 2015). When potential recruits replace the time they usually spend with friends and families with radical texts instead, the Westerners are often further radicalized and isolated.

After isolating recruits, ISIS members often encourage Westerners to communicate with them via more private means, such as calling them on the telephone or sending encrypted messages. These more private conversations are usually where recruiters can answer questions and give details about illegal activities that can be discussed with less likelihood of alerting law enforcement or the intelligence community. Once a more private conversation begins, the recruiters often try to suggest that Westerners join ISIS in practice instead of just accepting the ideology (Berger, November 9, 2015). If the recruit officially expresses interest in joining ISIS, other ISIS members conduct an interview utilizing encryption software, proxy servers, and messaging services. The three interview tools allow ISIS members to know what a recruit looks like and to ask him or her questions in order to determine if the Westerner is actually a spy (Masi, September 8, 2014).

To better understand the issues that encryption creates for the intelligence community and law enforcement, one should observe the legal debate that stemmed from the ISIS-inspired mass shooting in San Bernardino, California on December 2, 2015. Even after the Federal Bureau of Investigation (FBI) retrieved the iPhone of one of the shooter’s, the agency could not guess the PIN code needed to access the locked device.
When the FBI requested for the Apple Corporation to develop special software to bypass the code to retrieve the information inside the device, the company refused. Without the PIN code, the information inside the cell phone was encrypted and unusable for the FBI. The government’s difficulty to retrieve the information, although they possessed the smart phone, reveals the security of encryption and locked devices. Like Apple, Google promotes default encryption on its Android devices, and a popular messaging application called WhatsApp “has doubled-down on encryption and has even introduced secured video chat” (Selyukh, 2016).

Communication that occurs through encrypted means is often referred to as “dark space” communication. United States Representative Michael McCaul, Homeland Security Committee chairman, asked Michael Steinbach, FBI counterterrorism division assistant director, in a hearing if the federal government knows how much dark space communication is occurring. Steinbach responded, “No, we don’t and that’s the problem – the ability to know what they’re saying in these encrypted communication situations is troubling” (Sanchez, 2015). ISIS members understand the extreme complexity and security of communicating in dark space. The use of encrypted messages and videos, as well as the use of PIN code protected devices, allows IS to safely recruit Westerners and discover more about them.

ISIS members use past knowledge as well as the Westerners’ personality traits in order to identify how the potential recruits can be most useful to the jihadist cause. A wealthy teenager, for example, may be able to afford to purchase a plane ticket and travel to the Middle East in order to battle alongside ISIS fighters. Recruits who are less wealthy may not be able to travel to the Middle East, but they can perform lone wolf
attacks in their home countries. As stated by Franz (2015) and Yu and Haque (2016), people from numerous races, nationalities, and socioeconomic classes are interested in ISIS for numerous reasons. Recruiters are trained to utilize recruits in the most efficient manner possible. Members of ISIS ensure recruits, whether they can travel to the Middle East or not, that they can cause extreme damage to infidels no matter the new radicals’ circumstances. That is one of the reasons attacks occur worldwide (Berger, November 9, 2015).
Chapter 5: Counterterrorism Efforts

Although the federal government largely understands the target audiences of ISIS social media accounts, legislators and agencies often disagree on the best countermeasures to combat jihadist recruitment. Two of the major issues in combating ISIS recruitment are constitutionality and effectiveness. The government’s responsibility to adhere to the Constitution, though appropriate, hinders the number and scope of policy options that can be implemented to reduce the effectiveness of ISIS propaganda and recruiting. This chapter discusses the constitutional issues of censorship, addresses numerous relevant policy options to limit ISIS radicalization, and reviews the successes and limitations of those policy options.

The free speech clause in the First Amendment of the United States Constitution declares that the government can only limit speech if it poses a clear and present danger. Supreme Court Justice Oliver Wendell Holmes coined the clear and present danger test in 1919, but legal scholars argued the interpretation of “clear and present danger” until Brandenburg v. Ohio in 1969. In that case, the Supreme Court set the current precedent for clear and present danger when it overturned the conviction of a member of the Ku Klux Klan, who used inflammatory words against minorities, because his speech did not incite imminent lawless action (Eckholm, 2015).

Erik Eckholm, a journalist for the New York Times, explained the current constitutional issue with censoring ISIS. He explains that Justice Holmes described unprotected free speech with the example of yelling the word “fire” in a crowded theater because it could lead to imminent danger by causing a stampede. Eckholm continued, however, that “an article praising the merits of causing stampedes, even offering phrases
to shout, is not closely enough linked to an imminent, actual threat to be outlawed” (Eckholm, 2015). Although ISIS-sympathizers in the United States often state the merits of violence and even explain how to commit violence, their speech is protected under the First Amendment if it does not incite imminent lawless action or clear and present danger.

In February 2016, a trial began in a federal district court that may help more clearly define the government’s ability to prosecute Americans who utilize social media to incite terror. The FBI arrested a Missouri woman by the name of Safya Roe Yassin after she retweeted multiple posts from ISIS-sympathetic Twitter accounts. According to an article by the Wall Street Journal, “Ms. Yassin, a Muslim woman born in the U.S., has been charged with conspiracy and two counts of transmitting a threat across state lines, facing a maximum of 15 years in prison. She has pleaded not guilty” (Hong, August 12, 2016). Although there was no accusation against Yassin for planning any type of attack, the federal government claimed that she called for the murder of multiple military members and United States employees because some of the posts that Yassin retweeted contained the names and addresses of federal workers, among other personal information. One of the tweets included the phrase “Wanted to kill” (Hong, August 12, 2016).

The federal government utilized a legal statute against Yassin that prohibits interstate communication that has “any threat to injure” (Hong, August 12, 2016). Yassin’s public defender requested that the case be dismissed under the First Amendment since the defense viewed the language of the government’s statute as vague and overly broad. One reason Yassin’s case may be important for the future of ISIS-related social media accounts is that it could define how the federal government interprets retweets.
Since Yassin did not write the tweet herself, her attorneys argue that it is not a direct threat (Hong, August 12, 2016). In order to better prepare for trial, on April 11, 2017 Yassin and her attorneys waived Yassin’s right to a speedy trial and requested to reschedule the trial for a later date. At the completion of this thesis there were no other updates available (“USA v. Yassin,” 2017).

The United States can continue using the above statute to combat ISIS-sympathetic posts on social media from Americans, but the Yassin case could determine if the statute also refers to retweets. The government does not largely limit speech, but new constitutional questions continue to arise from the federal attempts to curb certain communication on social media.

A House Energy and Commerce subcommittee meeting in November 2015 emphasized the limits to government censorship. When asked if the Federal Communications Commission (FCC) could shut down terrorist websites, former FCC Chairman Tom Wheeler said, “We cannot underestimate the challenge. I’m not sure our authority extends to [shutting down the websites], but I do think there are specific things we can do” (Trujillo, 2015). Wheeler then stated that the FCC can urge technology companies to fight against certain profiles and users, but the chairman declared that the government will not enforce the removal of jihadist online users against the will of social media companies (Trujillo, 2015).

In January 2016, members of the Obama administration and other top officials traveled to California in order to urge technology companies to work with the federal government, as Wheeler suggested above. High-ranking officials such as Director of National Intelligence James Clapper, FBI Director James Comey, Attorney General
Loretta Lynch, and members of Obama’s staff met with the executives of online companies to share ideas on how to fight online recruitment and radicalization. One of the goals of the meeting was to discuss how to “help others to create, publish and amplify alternative content that would undercut” (McKitterick, 2016) ISIS. The list of technology companies present at the meeting included Google, Apple, Microsoft, LinkedIn, Twitter, and Facebook. The companies claim to remove pro-terrorist content whenever it appears on their websites, but the corporations also noted that they aimed to limit interference with language that could be argued as protected under the First Amendment (McKitterick, 2016).

Critics could argue that it is unethical for the federal government to become involved in telling social media companies how to respond to illegal activities, but no court has deemed the practice illegal. Furthermore, federal agencies are not mandating companies to monitor or report in any way. Instead, the government shares tactics that could aid the companies in monitoring and removing certain language from social media websites. Thus, the companies have the power to choose whether or not to listen to the advice.

Many critics still deride the practice as pointless. Some critics claim that whenever a social media company suspends an ISIS or ISIS-sympathetic account, someone creates another jihadist account to replace it. Some refer to the removal practice as “whack-a-mole” because, like in the arcade game “Whac-a-Mole,” every time a problem is taken away, another appears. Brookings Institution researcher J.M. Berger, however, claims that the “whack-a-mole” critique is invalid (Berger, April 2, 2015).
Berger, along with technologist Jonathon Morgan, collected data from millions of Twitter accounts, thousands of which belonged to ISIS supporters. According to Berger, Twitter suspended tens of thousands of ISIS-related accounts beginning in September 2014 (Berger, April 2, 2015). In response, ISIS members and sympathizers created dozens of accounts that remained dormant until Twitter suspended active accounts. Even as they lost many accounts, pro-ISIS users utilized various tactics to maintain their audiences. Jihadist Twitter users often place a hashtag in the description of new accounts. Similarly, a new account by the same user often has the same profile picture as the suspended account. In order to ensure that followers know the new account is legitimate, the new account will often include sequential numbers in the Twitter name. For instance, if Twitter deleted an account called “Jihadist,” then an account called “Jihadist 2” with the same profile picture would replace it. Since pro-ISIS users do not know if or when Twitter will delete their accounts, they sometimes encourage their followers to search for accounts with the same hashtag in the description, with the same profile picture, and/or the same name if Twitter removes current accounts from the website (Parrish, 2016).

Although new accounts appeared during September, the number of new accounts ISIS-sympathizers created after the first month decreased as the amount of suspensions continued to increase. As a result of Twitter suspending more ISIS profiles than ISIS creates in response, less people are exposed to ISIS propaganda and recruitment on the website (Berger, April 2, 2015).

A reduction in pro-ISIS accounts causes opposing users to overwhelm much of the remaining ISIS-sympathizing accounts with spam. One example of spamming can be seen in the flooding of ISIS hashtags with anti-ISIS information. Anti-ISIS users tweet
using extremist hashtags approximately five times more than pro-ISIS accounts.

Although many anti-ISIS accounts attempted to spam the terrorist group before September 2014, the uptick in account suspensions allowed anti-ISIS activists to severely overwhelm the terror organization’s jihadist propaganda on Twitter (Berger, April 2, 2015).

By April 2015, approximately 10 percent of tweets from pro-ISIS accounts aimed at rebuilding followers, through advertising and tagging former followers, rather than focusing on the goals of recruiting, radicalizing, and disseminating propaganda. Additionally, creating new accounts and waiting for new followers takes time away from recruitment efforts. Private social media companies that directly suspend pro-ISIS accounts devastate ISIS efforts. Other online companies contribute to the fight as well (Berger, April 2, 2015).

To proactively protect themselves against any lawsuits based on discrimination or freedom of speech, social media companies include reasons for account suspension in their terms of use or other policy documents. Twitter says in its policies that “users may not make threats of violence or promote violence, including threatening or promoting terrorism” (Mastroianni, 2015), and Facebook outlaws any content in support of violent, criminal, or terrorist activity. Cyberwarfare expert David Gewirtz explained that many companies utilize analysis software, artificial intelligence, and manual research to find users who violate policies. Social media companies also allow other users to report activity that could go against the policies of the website in question (Mastroianni, 2015).

Two benefits governmental entities have when engaging with social media companies are the fact that the websites are open to the public and that private companies
must comply with the government during criminal investigations. Since social media
websites are open resources, governmental entities can take advantage of some of the
same tools that companies like Facebook and Twitter use to police themselves
(Mastroianni, 2015). For example, the Secret Service used tracking technology in 2015 to
perform open source monitoring of different social media websites in an attempt to
uncover terror threats to the Super Bowl (Swanson, 2015).

When private companies and government entities monitor social media websites,
however, some issues arise. Among these issues are the volume of material, the identity
of the user, and the seriousness of the post. More than one billion people use Facebook
every day, in addition to people on other social media websites, and they do so in
numerous languages and with numerous online abbreviations. For these reasons, it is
difficult for the federal government to identify every risk, despite the technology
available. Even if a comment is threatening, it may or may not be posted under the actual
name of the user. One of the San Bernardino shooters, for example, posted about her
radical views through an alias account. In addition to these issues, technology cannot
always distinguish the seriousness of a threat or whether or not a post is sarcastic. Even
though the federal government has access to public information, monitoring all of that
information is still difficult for intelligence agencies (Mastroianni, 2015).

One positive aspect that helps the federal government find needed information,
however, is that companies must assist law enforcement in criminal investigations.
During a criminal investigation, government agents can present a warrant to require a
company to overturn relevant information if the government has probable cause. If the
company refuses, the government can apply for a warrant to receive such information from the website (Mastroianni, 2015).

Companies, however, could be placed in a difficult situation when working with the government on a criminal investigation. Gewirts stated, “How do you separate a high-vitriol comment in the heat of an election season from legitimate threats” (Mastroianni, 2015)? Social media companies may struggle to decide if certain comments by one of their users is threatening enough to reveal to the government, knowing that if people think that they provide the government personal information, customers may no longer use that service (Mastroianni, 2015).

Fortunately for social media companies, however, they are not alone in the private sector fight against ISIS. Jigsaw, a Google think-tank, recently developed a project known as Redirect. The project utilizes targeted advertising to coax potential ISIS recruits towards anti-jihadist material. If someone searches the phrase “Islamic martyrdom” on Google, for example, he may find ads that are linked to anti-ISIS videos. Often the titles of the ads are ambiguous, so potential recruits may think the advertisements are pro-ISIS propaganda. Within the first eight weeks of the program, Google redirected approximately 300,000 people who used the search engine to find pro-ISIS information. The redirected Google users watched about 425,000 minutes of the independent anti-ISIS videos that Redirect advertised (Farrow, McHugh, and Connor, 2016).

Redirect can directly contribute to fighting radicalization. For instance, if a potential recruit learns about ISIS on social media, he may also turn to Google to continue his research on the terrorist organization. If Redirect advertisements help change
the potential recruit’s view of jihadists, he is less likely to be drawn to ISIS-related social media accounts than he would have if he was still sympathetic to the caliphate. Viewing an anti-ISIS video, whether intentionally or unintentionally, can be effective in fighting radicalization, but the news media could be unintentionally hindering the process.

In an NBC News article that discusses Redirect, the authors make an ironic statement. They wrote, “The key is subtlety. A disaffected young person wondering if ISIS is the answer to their problems would immediately dismiss a video with a warning from the Department of Homeland Security” (Farrow et al., 2016). Although that statement is likely true, the irony falls on the word “subtlety.” It is likely that heavy reporting about Redirect from news agencies such as NBC could actually have a negative effect on the program. If ISIS recruiters or the directors of ISIS-sympathetic social media accounts become aware of Redirect, they could encourage their audiences to use different search engines instead of Google. Additionally, if Redirect partners with other companies like YouTube for more targeted advertising, ISIS could simply avoid using those platforms as well. If search engine companies like Bing and Yahoo collaborated together to create programs similar to Redirect, however, ISIS recruits would not have many other search engine options for research. Nevertheless, in order to be more successful in subtly exposing potential recruits to anti-ISIS propaganda, it may be in the best interest of search engine companies like Google to keep programs such as Redirect relatively unknown to news media despite the favorable attention such outlets may bring to both the company due to its efforts and ingenuity.

Private companies benefit the online fight against ISIS, but the federal government serves as the official line of defense for the American people. In June 2013,
however, a former National Security Agency (NSA) contractor named Edward Snowden revealed to the *Guardian* newspaper that the United States government, in his opinion, overreached its limits through numerous projects. One of the projects was the collection of telephone records from millions of United States citizens (“Edward Snowden,” 2014). Under the program, the government could, for instance, identify suspected ISIS sympathizers and track who they communicate with over the telephone.

Outrage over the government collection of metadata sparked conversation throughout the country. Many people claimed that the unwarranted collection of information from American citizens violated the Patriot Act and even the Fourth Amendment, which protects Americans against unreasonable searches and seizures. The Obama administration claimed that the program was a legal counterterrorism measure that does not violate the rights of citizens. In May 2015, a federal appeals court ruled against the federal government, stating that the telephone metadata collection did violate the Patriot Act. The judges later sent the case to a lower court to determine whether the collection program is also unconstitutional (De Vogue, 2015).

The lawsuit came just one month before the passage of the USA Freedom Act, which ended bulk collection of telephone records and added limitations to government collection. Ending the telephone metadata program increased the difficulty of counterterrorism for the intelligence community, but it also reduced the controversy over NSA surveillance (Hattem, 2016). Now the government must depend more heavily on other counterterrorism programs to identify potential terrorists that may have been identified through the former program.
In order for the federal government to more actively combat online propaganda, the State Department’s Center for Strategic Counterterrorism Communications, established by the Obama administration in 2011, began producing propaganda parody videos. A 2014 YouTube video, for example, entitled “Welcome to the ‘Islamic State’ land (ISIS/ISIL)” accumulated thousands of views. It included graphic images of different types of killings utilized by ISIS. In the video there is no narrator, but phrases and words appear on screen urging viewers to commit jihad. Towards the end of the video, the ominous music that had been playing ended, and the tone of the video changed as the words “Think again, turn away” appeared on screen. Additional videos and posts designed to dissuade potential radicals were across numerous social media sites through the “Think Again Turn Away” campaign. The campaign includes the languages English, Arabic, Somali, and Urdu with different videos for each language. Included in the campaign are personal testimonies of former radicals who realized jihadism is morally wrong. It also included news coverage of terrorist deaths throughout the world. State Department officials use social media websites to disseminate anti-radicalization propaganda in the same way terrorist organizations utilize the same sites for the opposite reason (Hansen, 2014).

Although the campaign attempts to scare would-be radicals from terrorism, some social scientists claim that it could have the opposite effect. Dr. Jeff Victoroff, a neurology and psychiatry professor at The University of Southern California who studies terrorism psychology, warns that sometimes such campaigns have the opposite effect. Victoroff stated, “If you challenge a young adult, particularly a male, with the fact that something might be especially difficult or challenging, you’re just exciting them”
(Hansen, 2014). Also, if ISIS sympathizers notice that the “Think Again Turn Away” posts come from accounts they do not trust or know to be linked to the State Department, then the posts may not have much effect on them. Just as law-abiding citizens respond to the authority of police officers, Victoroff stated that ISIS sympathizers will respond to the authority of Muslim leaders. Thus, Victoroff argues, if the United States notices that someone is possibly becoming radicalized, then government officials should reach out to that person through an imam that he trusts in order to rid that person of his interest in radical Islamic terrorism through a positive approach to Islam (Hansen, 2014).

According to a recent *Wall Street Journal* article entitled “U.S. Revamps Line of Attack in Social-Media Fight Against Islamic State,” the federal government realized that the “Think Again Turn Away” campaign was largely ineffective. Besides the fact that ISIS sympathizers often tried to ignore the campaign and that the videos sometimes excited the audience about extremism the government also noticed that the “Think Again Turn Away” posts were simply unpopular. For example, a video released by the State Department in September 2016 about an ISIS defector received approximately 500 views over the course of two months. Comparatively, ISIS execution videos often receive tens of thousands of views within hours of being posted (Hong, 2016).

In response to the ineffectiveness of the “Think Again Turn Away” campaign, the Department of Homeland Security (DHS) announced in July 2016 that it would dedicate $10 million of its budget for an anti-extremism federal grant. The grant is being utilized by public and private entities nationwide, such as local governments and nonprofits, in order to disseminate the anti-terror message. Federal government officials invited Facebook and other technology companies to develop competitions between college
students worldwide. The competition requires students to develop their own campaigns to assuage radicalization. DHS recognizes that young adults observe social media profiles of others that are close in age. In the spring of 2016, 54 universities competed compared to 45 in the fall of 2015. Although many of the results appear positive to DHS, such as the 45 percent drop in pro-ISIS Twitter posts since June 2014, there is no way to measure whether or not less people become radical. For example, it is possible that despite the reduction of pro-ISIS tweets, even more people have radicalized since 2014 than in years prior. Nicole Hong, the journalist who wrote The Wall Street Journal article, stated that it is nearly impossible for the government “to quantify the number of people who were convinced not to join a terrorist group. For that reason, some experts say the government should be wary of devoting too many resources to this area and focus on military efforts with more tangible results” (Hong, 2016).

The ineffectiveness of “Think Again Turn Away” could negatively affect a bill sponsored by United States Representative Chuck Fleischmann that passed in the House of Representatives in April 2016. Since its passage, the bill, known as HR 4820, died in committee in the Senate. If passed, HR 4820 would have required the Department of Homeland Security to utilize the testimonials of former radicals in foreign terrorist organizations, such as the videos of former jihadists in the “Think Again Turn Away” campaign who said that extremism is morally wrong. Fleischmann hoped that the testimonials would help potential ISIS recruits understand that life in the caliphate is not desirable (Daly, 2016). State Department officials, however, already use testimonials in their campaign without a law requiring the department to do so. If the bill became law, it would likely not benefit national security in the way Fleischmann hoped. Terrorist
testimonials in the State Department campaign did not reap the outcome that federal officials desired, and requiring another federal agency to begin a similar project would likely also be ineffective.

Two senators pushed another congressional attempt at fighting ISIS online in 2015. Senator Richard Burr, chairman of the Senate Intelligence Committee, and Senator Dianne Feinstein, a ranking member of the committee, sponsored a bill called “Requiring Reporting of Online Terrorist Activity Act.” The bill required social media websites, and some other technology companies, to alert law enforcement of “any terrorist activity” (Nasr, 2015). The bill came in response to the shootings in San Bernardino, California, which is Senator Feinstein’s home state. She emphasized that the bill would not require companies to change how they monitor criminal activity on their websites. Instead, it simply requires them to report terrorist activity when they find such information (Nasr, 2015).

Senator Ron Wyden opposed the bill by saying, “I believe it will undermine [collaboration between the government and private companies] and lead to less reporting of terrorist activity, not more” (Nasr, 2015). Each technology company is able to monitor its website however it chooses. Although Senator Feinstein claimed that there would be no extra obligations on companies except reporting terrorist activity, many companies could see the reporting as tedious because they would have to then participate in an investigation, possibly answer questions from law enforcement, and many other logistical requirements. Wyden suggested that, in order to avoid tedious collaboration with law enforcement, some companies may simply lower monitoring standards so they will not find as much terrorist activity (Nasr, 2015).
Additionally, Wyden made two other points against the legislation. The senator noted that FBI Director James Comey did not endorse the legislation proposal when Feinstein asked him about it at a Senate Intelligence Committee hearing on July 8, 2015. When asked about the bill, Comey responded, “It’s an interesting idea. I do find in practice that they are pretty good about telling us what they see” (Nasr, 2015). Comey’s response seemed to suggest that the bill is unnecessary since technology companies are already adequately reporting terrorist activity.

Wyden’s other point countered an argument many people made in support of the bill. Supporters argued that technology companies already must report child pornography if it appears on their websites, and many people do not see a difference in mandating the reporting of terrorist activity. When a reporter for Oregon Public Broadcasting asked Wyden about the argument, the senator replied, “First of all, I think that there are different standards with respect to child pornography, different standards under the law” (Norcross, 2015).

Despite Wyden’s vague answer, his point is valid. As discussed earlier in this paper, the First Amendment does not protect against actions that pose a clear and present danger. For example, if a jihadist posted on the Facebook wall of another asking for the assistance of killing a police officer at a certain place and time the next day, the first jihadist would be breaking the law. Facebook could then simply shut down the account and inform the police department if the company so chooses. Although the illegal plan occurred on Facebook, the illegal end result of killing the officer did not. On the other hand, if a man posted child pornography on another man’s Facebook wall, the social media company would shut down the account, and the law mandates that Facebook must
inform law enforcement of the pornography. In this situation, the pornography was the illegal end result. The pornography would not be a stepping-stone for another more heinous crime. If the man, instead, made a Facebook post about his possession of child pornography, the website could delete the account and choose whether or not to alert the proper law enforcement agency.

Burr and Feinstein introduced the bill amid extreme criticism from numerous civil liberties advocates. Ultimately, the Legislative Branch did not enact the measure by the end of the 114th Congress. The Congress, therefore, cleared the legislation from the books (“S. 2372,” 2015). Although the legislation failed, it began conversations that can be utilized in future legislation used to combat ISIS on social media.

Senator Wyden’s criticisms of the bill were legitimate, but his alternative legislation idea is also flawed. Wyden desires to introduce legislation to give intelligence agencies “more resources and personnel so they know where to look for terrorist content online and who to watch, and can ensure terrorist activity is quickly reported and acted upon” (Nasr, 2015). One of the main issues with Wyden’s legislation idea is that each intelligence agency already has the opportunity to request Congress to increase funding for resources and personnel. A blanket increase in resources and personnel for the intelligence agencies that actively fight ISIS online may be unnecessary and ineffective.

Representative Ted Poe approached the problem differently, sponsoring the Combat Terrorist Use of Social Media Act of 2015, HR 3654. Poe’s legislation simply required the Executive Branch to provide a plan to necessary congressional committees to fight the presence of terrorists on social media in no more than 90 days. The bill,
however, failed in the 114\textsuperscript{th} Congress because while it passed the House, the Senate took no action (\textquotedblleft H.R. 3654,\textquotedblright 2015).

If enacted, the legislation would have forced the Executive Branch to work with the intelligence community and congressional committees to inform necessary parties of the dangers of terrorist use of social media, summarize the multi-agency approach to fighting terrorism online, and explain future plans to disrupt online radicalization efforts. The bill would also require the report to be unclassified, which would undermine the usefulness of the legislation (\textquotedblleft H.R. 3654,\textquotedblright 2015).

Some current and future plans to fight ISIS may likely be confidential due to the sensitivity of the information. If Representative Poe did not include the language about mandating the report to be unclassified, or if other lawmakers amended the legislation, the president would be required to report a detailed and confidential plan to congressional committee members who hold security clearances. An unclassified report, however, would undermine the value of the legislation. The current Congress has the opportunity to write legislation that mirrors Poe’s bill that would require President Trump to provide a plan to fight social media terrorism, but the language about the unclassified report should be removed.

Military action, however, has been effective in combating the Islamic State, and some of the tangible results of military efforts could directly affect ISIS presence on social media. Russian and Western attacks destroyed many of the ISIS-controlled oil fields throughout the Middle East while Kurdish and Iraqi ground troop advances forced ISIS militants from functional oil fields. When ISIS militants retreated from those formerly held areas, they also left behind many of the people in those regions. Since ISIS
receives much of its money from oil fields and taxing people within regions it controls, militarily overtaking ISIS-controlled areas financially hinders the terrorist group. Mosul, for instance, is the final significant ISIS stronghold in Iraq, and residents of the city reported that ISIS can no longer pay the thousands of fighters that remain in the city (Gutteridge, 2017).

Due to the lack of funds, ISIS must cut the budget in many different areas. Required cutbacks mean the group will likely not be able to pay its recruiters nearly as much as in the past. Fewer recruiters and less resources to recruit could hinder the recruitment process. Additionally, ISIS will not have funds to pay film editors or purchase equipment for high quality propaganda videos.

Some ISIS fighters in Mosul, for instance, have already proven that they are willing to disobey commands in order to be paid. ISIS commanders ordered fighters in Mosul to use civilians as human shields during the war. However, some ISIS soldiers reportedly smuggled out families in exchange for money. Sometimes the payment is as little as £15 (Gutteridge, 2017). As the Islamic State loses funding to pay its social media and recruitment employees, they are also suffering defeats that could frighten otherwise susceptible audiences.

United States agencies utilize the misfortunes of ISIS to add to the success of the Global Engagement Center (GEC). The GEC serves as an interagency body with the mission to counter extremist propaganda online. Although the State Department houses the GEC, numerous government agencies, including the intelligence community, contribute funding and personnel to the program. Additionally, the head of GEC has authority to hire nongovernmental experts. Some experts, for example, can inform GEC
of the ISIS financial situation while other experts can recruit ISIS defectors to tell their stories. Former GEC director Michael Lumpkin claimed that although the agency is receiving success due to its interagency approach, it is facing setbacks due to the regulations of each agency. Lumpkin said, “Each department has got its own rules and regulations and review procedures, and we just need to work through. It’s not that it’s not working, it’s just frankly, it’ll take some time to work through the process” (Wong, 2016). Representative Brad Sherman of California stated, for example, that the State Department must clear a tweet through 14 levels of review before it can be posted and tweets from State Department funded entities must clear six levels of review. Such regulations can severely hinder the GEC social media campaign (Wong, 2016).

President Trump, however, seeks to reduce such regulations. On February 24, 2017, the president signed an executive order that requires each federal agency to develop a task force that will identify regulations that may need to be reduced or removed. The president stated, “Every regulation should have to pass a simple test. Does it make life better or safer for American worker or consumers? If the answer is no, we will be getting rid of it – and getting rid of it quickly” (Horsley, 2017). If the State Department and other agencies deem that their social media regulations are hindering the GEC from effectively combating ISIS propaganda, such regulations could be reduced or removed. ISIS-sympathetic social media accounts make numerous posts every day. If the United States has too many regulations for the GEC to make a significant amount of posts, the program may not be as successful as it would be without the regulations.

Another government tactic that directly influences social media is the FBI undercover sting operation. The FBI utilizes undercover operations in approximately two
thirds of prosecutions of people convicted of supporting ISIS, which used to only be a practice used only when no other option seemed feasible. FBI officials stated that the anonymity of social media websites, like when ISIS-sympathizers utilize alias usernames in order to give support for the terrorist group, caused the uptick in undercover stings. According to *The New York Times*, the FBI increased its use of undercover sting operations in 2016, and it employs “agents and informants to pose as jihadis, bomb makers, gun dealers or online ‘friends’ in hundreds of investigations into Americans suspected of supporting the Islamic State” (Lichtblau, 2016). FBI agents often comb through social media websites to look for people who support ISIS or threaten acts of terrorism. Once someone is deemed as a threat, an undercover agent will contact the person (Lichtblau, 2016).

In order for the FBI to build a strong case against suspects, undercover agents nationwide aided suspects in activities such as locating bomb targets and buying weapons. These actions earn the trust of the suspect and allow the FBI to track terror plots. Michael Steinbach, leader of the FBI national security branch, said, “We’re not going to wait for the person to mobilize on his own time line” (Lichtblau, 2016).

Since counterterrorism officials claim that ISIS calls its followers to attack people who disagree with the caliphate just days or weeks after the followers’ radicalization, the FBI also use undercover operations to quickly track and foil terrorist plots. If the FBI utilized practices such as wiretapping, for example, it would need wait for a judge to sign a warrant. Additionally, if the judge did not sign the warrant, the FBI would need to begin a new plan. Undercover operations, however, are under the authority of a team of FBI supervisors and Department of Justice prosecutors. For that reason, stings can
usually begin much more quickly than operations that require a warrant (Lichtblau, 2016).

Critics of the practices, however, claim that the FBI is still illegally entrapping suspects. Some Muslim leaders, defense attorneys, civil rights advocates, and others argue that the FBI contacts susceptible people and coerce them into making statements or performing actions that may not have happened without the coaxing. Michael German, a former undercover agent, agreed, claiming that the FBI is “manufacturing terrorism cases” because, out of the suspects in recent prosecutions, “these people are five steps away from being a danger to the United States” (Lichtblau, 2016).

In an attempt to curb criticism and build a legal case against suspects, FBI officials explained that they followed the agency’s internal guidelines to use the least intrusive possible methods. Besides the anonymity of social media, the officials claimed that the use of encrypted messaging by ISIS-sympathizers caused a need for undercover operations. Additionally, undercover agents often give suspects an opportunity to back out of a terror plot. An example of a suspect who received an opportunity to leave the situation is James Medina of Miami. Medina told an undercover agent, who posed as a bomb supplier, that he wanted to bomb a synagogue. In response, the agent spoke to Medina about his reasoning for wanting to bomb the synagogue, and then the agent said, “You need to be sure, brother. You know you don’t have to do any of this” (Lichtblau, 2016). Medina confirmed his dedication, he received a fake bomb, and then the FBI arrested him as he approached the synagogue. Due to the processes that the FBI follows, no judge has deemed the undercover practices as entrapment (Lichtblau, 2016).
The FBI also utilizes resources and personnel to identify and kill ISIS hackers. The FBI identified approximately twelve ISIS computer experts, known as “the Legion” (Goldman and Schmitt, 2016) that pose a serious threat to national security. Junaid Hussain, who died in a drone attack, helped hack a computer system and release the personal information of more than 1,300 American government employees. “In March 2015, his group posted the names and addresses of service members with instructions: ‘Kill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking they are safe’” (Goldman and Schmitt, 2016). FBI officials convinced the federal government that law enforcement should not combat the Legion alone. In 2016, FBI officials increased monitoring of ISIS suspects throughout the United States while military overseas shifted focus specifically to members of Legion. The military killed some members of the group, which decreases the likely amount of hacking that will take place in the immediate future (Goldman and Schmitt, 2016). Continued military efforts against the Legion and similar hackers will decrease the amount of substantive material that can be found on pro-ISIS social media accounts. For instance, if ISIS Twitter accounts no longer posted lists of the addresses of federal employees, fewer officials will be specifically targeted due to their positions within the government. In addition to the military strikes against the Legion, the Department of Defense (DOD) also destroyed many overseas facilities that ISIS used to produce propaganda videos and messages that the group posts online. Military efforts continually weaken ISIS social media campaigns while the DOD also fights the terrorist group online (Parrish, 2016).

As the Defense Department continued to directly combat ISIS overseas in 2016, the department also limited its cyberwarfare tactics against the group due to concerns
within the intelligence community. The main concern came from the possibility that blocking the Islamic State’s internet connection could hinder intelligence gathering from the group (Associated Press, 2016). Even if the military did block all internet connection from certain ISIS strongholds, it would not end the social media problem. Since Westerners control many of the pro-ISIS social media pages, propaganda and recruitment could continue throughout the world even without internet in ISIS strongholds. The number of Western pro-ISIS social media recruiters, however, will likely decrease due to the aforementioned lack of funding.

Another reason to not completely disrupt the internet connections in ISIS strongholds, according to a cybersecurity expert named James Lewis, is that it could negatively affect civilian internet networks in those areas for those trying to inform news media of the situation, contact family members, etc. Furthermore, disrupting internet connections through targeted bombings could put citizens in even more danger (Associated Press, 2016). Due to the negative externalities, military personnel may find more success in fighting online recruitment and propaganda through other means.

Two other means the DOD utilizes in the fight against ISIS on the internet are the Digital Engagement Team (DET) and web operations cell. Some of the eleven members of the DET are native-born Russian, Dari, Arabic, Farsi, Pashto, and/or Urdu speakers. Members of the team represent the DOD in countries that speak their native language in news media and online. The DET helps disseminate anti-ISIS messages from opposing forces in different countries (Parrish, 2016).

The web operations cell disrupts ISIS propaganda, displays defector testimonies, and mobilizes ISIS opponents. In order to disrupt propaganda, the web operations cell
ensures the consistency of anti-ISIS messages of the DET, State Department, and other government entities. The 120 person web operations cell team also researches ISIS morale and propaganda techniques. An unnamed web operations official told Department of Defense News that the ISIS presence on social media changed in 2014. The source stated,

“In 2014, when ISIL took Mosul, they maintained a dozen official [social media] accounts that said ‘We are ISIL.’ They also relied on several dozen ‘fanboy’ accounts which could boast upwards of 100,000 followers. So in terms of official messaging and in terms of unofficial support messaging, ISIL could quickly and easily reach hundreds of thousands of supporters and really the whole world with minimal effort. But since 2014, a combination of aggressive suspensions from social media companies, attrition and decrease in morale in ISIL’s own ranks – which we’ve seen play out and we’ve seen them express this; that there’s a loss in morale – and the third element would be counter-efforts from both governmental and nongovernmental entities. A combination of those three has gradually degraded ISIL’s footprint, ISIL’s ability to quickly and easily reach the masses” (Parrish, 2016).

In order to add to the degradation of ISIS social media presence, the web operations cell utilizes testimonies of defectors, similar to the State Department’s “Think Again Turn Away” campaign. Unlike the largely ineffective State Department program, however, the testimonies focus less on the morality of ISIS and more on the trustworthiness of the group. Out of the defectors who speak to the web operations cell, for instance, the main reason they leave ISIS is because the terrorist group lied about who
recruits would fight against. ISIS members told many recruits that they would be fighting
the Syrian regime when they joined the terrorist group, but instead they would often fight
against other rebel groups in the region. Additionally, defectors complained that ISIS
media fabricated numerous aspects of the terrorist group such as its popularity in the
region and the amount of food that fighters received (Parrish, 2016).

In order to mobilize ISIS opponents in different regions, the web operations cell
gives factual information, such as who ISIS fighters will actually be fighting, to anti-ISIS
rebel groups on Twitter. The rebel groups and the web operations cell can use the
information to dissuade potential recruits from joining ISIS (Parrish, 2016). By utilizing a
three-pronged web operations cell, the DET, and physical military missions, the DOD
attempts to actively decrease the ISIS social media presence. Recent reporting from the
Associated Press (AP), however, suggests that the web operations program is highly
flawed in multiple respects.

An AP investigation gathered testimonies from former and current employees of
the web operations cell that revealed details of many of the flaws. One of the serious
issues within the program is that the DOD hired multiple people as civilian Arabic
specialists who did not speak fluent Arabic. The AP report states that many of the
specialists could not speak Arabic fluently, did not hold counterterrorism experience, and
had very little comprehension of Islam. These shortcomings hurt DOD efforts to
deradicalize potential recruits since the specialists could not compete with the knowledge
of ISIS recruiters. Some of the mistakes are so egregious that pro-ISIS accounts would
identify and ridicule American efforts. One example of a common mistake by translators
working for the DOD is that they repeatedly confused the phonetically similar Arabic
words for “authority” and “salad.” The mistake led pro-ISIS social media accounts to mock the United States by making posts referring to “Palestinian salad” (Butler and Lardner, January 31, 2017).

Additionally, four current or former employees claimed that they personally witnessed web operations manipulate data in order for the program to appear more successful than it actually is. Employees reportedly attempted to implement independent investigators to oversee or assess data, but the DOD has yet to enforce such measures. Multiple contractors work to provide the data, and the web operations cell faced other issues with contractors in 2016 (Butler and Lardner, January 31, 2017).

In early 2016, the government held a bidding war for a counterpropaganda contract worth up to $500 million that would help the web operations cell in its counterterrorism efforts. After the DOD awarded the contract, the Naval Criminal Investigative Service (NCIS) spokesman Ed Buice announced to the AP that an investigation launched after a whistleblower alleged corruption in the decision of the contractor. The whistleblower claimed different types of corruption occurred simultaneously. For example, the whistleblower alleged that a contractor provided lavish dinners to officials who would provide the contract, and officials participated in routine alcohol consumption within an office where the DOD participated in classified projects. (Butler and Lardner, January 31, 2017).

Whether or not corruption took place, the web operations cell is still fraught with issues. Despite the problems within the web operations cell, the mission and multifaceted approach of the program could be beneficial if the government enforces proper oversight. President Trump promised an increase in military spending over the course of
his presidency (Butler and Lardner, January 31, 2017). Increases in spending could improve the web operations cell in multiple ways. If Arabic specialists, for example, receive better compensation, then the job would be more competitive. Increased competition could lead to better employees who know more about the Arabic language and culture. Additionally, the DOD could improve standards for their Arabic specialist prospects, such as multiple language fluency tests.

Multiple investigations from different branches of government, such as the NCIS and congressional investigations, allow government officials of different levels of experience and expertise to curb issues within problematic federal programs. Unlike “Think Again Turn Away,” the web operations cell may be highly effective if the DOD hires better leadership and language specialists to seek the original goal of the program. Due to the program’s multi-faceted approach and connection to other counterterrorism programs within the DOD, it is highly probable that the web operations cell could be successful if the military removes the project’s shortcomings.
Chapter 6: Conclusion

ISIS has an organized approach to propaganda dissemination, radicalization, and recruitment that is unprecedented by other terrorist organizations. The group’s international approach from multiple social media accounts serves as a serious challenge to the intelligence community.

When seeking a target audience, ISIS may focus on tribalism, such as Sunni versus Shiite or Arabs versus non-Arabs, in order to radicalize those who are most susceptible. Although ISIS recruiters are very talented in utilizing different tactics to radicalize different types of people, I assess that the lack of funding for recruiters and the actions of social media companies to remove ISIS-related accounts will continue to hinder the recruitment process.

Both public and private organizations have proven to be effective in meeting the challenge of radicalization and recruitment. Private social media and search engine companies implemented measures that successfully suspend pro-ISIS accounts quicker than they can be created and deradicalize potential recruits by rerouting internet searches to anti-ISIS materials. The companies should, however, limit the amount of information about their anti-ISIS strategies that they release to the public.

Governmental efforts have experienced numerous flaws, but they have been mainly successful. The federal government should continue to work with private companies to share strategies and information that assist both sectors in the fight against ISIS. In addition, the federal government should continue sharing tools with the private sector without forcing companies to use said tools. Although staying within the bounds of the United States Constitution will likely hinder America from catching every terrorist
who uses the internet, it also allows the government to respect the freedoms of the people it serves.

Intelligence agencies, with the help of the military, continue to successfully arrest and fight ISIS on social media in multiple ways. The web operations cell, however, must raise standards for leadership and language specialist in order to effectively combat ISIS by hiring highly qualified employees. If military intelligence programs fight social media online as the military fights them on the ground, the terrorist group will continue to weaken.

Although some efforts have either shown to be ineffective or flawed, the pressure on ISIS from American companies and the federal government has been largely successful in fighting radicalization efforts, incarcerating extremists, shutting down violent social media accounts, and defeating the terrorist group in physical battles.
Works Cited


<https://www.govtrack.us/congress/bills/114/hr3654>


<https://www.govtrack.us/congress/bills/114/s2372>


Yu, Seong, and Omar Haque. "Vulnerabilities among Young Westerners Joining ISIS."


Web.