Spring 5-18-2019

Radicalization through the Internet: How ISIS became So Successful and Why the United States Needs to Catch up

Ana Sofia Florez

Radicalization Through the Internet:

How ISIS Became So Successful and Why the United States Needs to Catch Up

Ana Florez
Aflorez2@fordham.edu
B.A International Studies, Middle East and North Africa Track
Fordham University, Lincoln Center Class of 2019

Thesis Advisor: Professor Christopher Toulouse
Seminar Advisor: Professor Claire Panetta

Table of Contents: **Page #**

Abstract:

It is no secret the Islamic State of Iraq and Syria, otherwise known as ISIS, has become one of the most dangerous and brutal terrorist organizations in modern history. In recent years the Islamic State has gained strength and followers from around the world. Individuals from other countries will leave their homes and families after contact through social media to travel to Syria and fight alongside the organization. This thesis provides insight on the dangerous implications ISIS's perfection on online recruitment and their successful radicalization tactics has. It will also provide an explanation as to why nations, specifically the United States have had so much trouble in weakening or eliminating ISIS's virtual footprint. I argue my position through an analysis of behavioral characteristics that are susceptible to online radicalization as well as a comparative case study explaining the critical differences with Al Qaeda and ISIS' extremist methodologies and public relations. Lastly, I highlight the multiple unsuccessful attempts the United States has done to counter the extremist virtual presence. With this thesis, one will get a better understanding as to why ISIS has forced nations to drastically change the way they fight terrorism.

Introduction

Al Qaeda, also known as Al Qaeda Central and Islamic State in Iraq and Syria, ISIS, are terrorist organizations that originated in the Middle East region. Al Qaeda was founded shortly after the Soviet Union invasion of Afghanistan in 1979. In 2006, Al Qaeda in Iraq, an Al Qaeda affiliate, broke away and officially formed a separate organization known as the Islamic State in Iraq(ISI). By 2013, the leader of ISI merged an extremist rebellion group, Jabhat al Nusra in Syria, officially changing its name to the now world renowned Islamic State in Iraq and Syria/Levant (ISIS/ISIL). Terrorists are non-state actors who engage in violence against noncombatants in order to accomplish a political goal or amplify a message. There are two distinct characteristics that distinguish terrorism to other forms of violence: first, it is aimed at noncombatants or non-fighters/civilians. Second, terrorists use violence for dramatic aims. Such as, instilling fear in the target audience, and creating a deliberate form of dread is what distinguishes terrorism and other forms of assaults or murder (Stern & Berger, 2015).

The evolvement of ISIL's recruitment tactics using social media compared to Al Qaeda's more regional and outdated recruitment tactics has altered the way countries counter terrorism. ISIS's form of propaganda has five distinguishable goals:

- To project an image of strength or victory,
- To excite those susceptible to violent tendencies by pairing extreme violence with a moral justification in the form of its alleged utopian society.
- To manipulate the perceptions of ordinary citizens in its enemies' lands to incite demand for military action, while at the same time planting doubt that such action can succeed.

- To place the blame for any conflict that does result on the aggression of Western governments and the incitement of "Zionists," people who believes in the development and protection of a Jewish nation in what is now Israel.
- To recast any military action against ISIS as an action against all Muslims, specifically by highlighting civilian casualties. (Stern & Berger, 2015, pg. 250)

Throughout this thesis my argument concentrates on how the development and easy accessibility to social media platforms terrorists have found a much easier way to recruit, specifically young adults to join their organization, and that this way of recruitment has challenged and forced the United States to change the way it counters terrorism. Unfortunately, the U.S has yet to discover an effective way to eliminate or even weaken ISIS's virtual footprint.

I begin with a breakdown of the behavioral characteristics susceptible for radicalization and the tools used to radicalize. As for my case study, I compare the formations of Al Qaeda and ISIS, along with the history of their rises and declines in power, and their increasing expertise, or lack thereof, in technology to form and release their propaganda. I decided to use Al Qaeda as a case of comparison to ISIS to prove the differences in terrorism strategy and to emphasize the measures taken by the United States after the 9/11 terrorist attacks, to the rise of ISIS, and the current struggle to erase ISIS's technological footprint. I will provide the counter terrorism/ radicalization policies used under President Bush and President Obama to give the reader an understanding as to why ISIS's virtual footprint continues to be such a pressing issue. I will explain two types of policies in my case study. First, counterterrorism policies are the policies implanted at the time to prevent another terrorist attack similar or potentially worse than the September 11 attacks. Second, counter-radicalization policies are tactics implemented to prevent

terrorist recruitment from within the United States and abroad. Lastly, the analysis section will provide my insight to the research conducted and its results.

Methods and Limitations:

For my literature review I narrow it into three articles and sections from Jessica Stern and J.M Berger's book ISIS: A State of Terror. I use these authors and their arguments because it is crucial to understand why social media and other internet messaging platforms have become such a popular hunting ground for terrorist recruiters as well as understanding the obstacles involved to counter act. Unfortunately, it is also very difficult to find policy reports that are free to use and therefore I was limited to very few and the report by The International Centre for the Study of Radicalization and Political Violence was the most reliable.

In terms of finding counter terrorism policies for the United States, it was easy to find the information below because it is now unclassified and open to the public. However, I found that in order to find current policies on the Trump Administration it is almost impossible. I was able to only find articles that assumed what President Trump would do but no official data. Lastly, although I accidentally came across a few propaganda videos through Facebook, I did not go out of my way to search for terrorist propaganda through the dark web nor their websites as it would put my computer at risk for virus and potential shutdown.

Literature Review

This literature Review will be based on the themes that explain the behavioral characteristics susceptible to radicalization and the tools used to radicalize, the plans for action and the obstacles involved. The scholarly sources voice different opinions as well as

commonalities as to how to go about combating online radicalization. In her 2015 article; *Terrorism, Communication and New Media: Explaining the new wave of Radicalization,* Cristina Archetti argues that there needs to be a much better understanding of strategic communication in today's social media in order to have a more effective impact on countering online extremism. The *Cyber Extremism: ISIS and the Power of Social Media* article by Imran Awan analyzes different social media platforms and concludes that there are seven key behaviors and motivations that allow ISIS to become so successful in online recruitment. I chose these two articles because they have a similar school of thought but have two different ways of approaching it. They both involve why someone becomes radicalized and what's is on the other side of the process. However, Archetti focuses on networks of relationships and Awan analyzes behavior characteristics. Both networks of relationships and behavior characteristics are crucial to understanding the importance and danger to online Radicalization. I will be dedicating a section to a policy report that attempts to find ways to counteract the extremist groups success via the internet. I also emphasize obstacles that contribute to the difficulty in countering online radicalization.

Behavioral Characteristics Susceptible to Radicalization and the Tools used to Radicalize

Imran Awan's *Cyber extremism: ISIS and the Power of Social Media* (2017) explains the results of a study that "analyzed 100 different Facebook pages and 50 twitter user accounts which generated over 2050 results and helped the author create a typology of seven key behavior characteristics and motivations." (Awan, 2017, pg. 1) These seven characteristics of whom are likely to be sympathizers as well as those recruiting is: cyber mobs, loners, fantasists, thrill seekers, moral crusaders, narcissists, identity seekers. Instead of summarizing each characteristic

in paragraph form I've decided to use the table the article provided which perfectly captures and explains each characteristic:

Table 1 Offender behaviour characteristics

Type	Characteristics	Cases on Twitter	Cases on Facebook	Total No of Cases
Cyber Mobs	Using social media platforms to create a mob mentality and urging others to fight for the Isis goal. This is done through group posts, videos and comments of hate directing groups of Muslim's to fight. Often personified through retweets, likes and views of specific Isis propaganda materials.	78	55	133
Loners	Often done through individual posts and comments. This individual is someone who is attracted to the Isis campaign but clearly is exposed to individual grievances and has a lone mentality.	51	65	116
Fantasists	Someone using social media platforms to fantasise over the Isis movement. In particular, these individuals have blurred the lines between reality and fiction and are making direct plea's to fight for Isis.	45	94	139
Thrill Seekers	People who are promoting Isis propaganda through videos and posts and forums. Indeed, some of these individuals claim to be directly using the Internet for online extremist purposes. These individuals are describing the sense of adrenaline rush they are receiving by watching and partaking in fighting on the battlefield whether online or offline.	85	98	183
Moral Crusaders	These individuals are talking about the moral duty to fight. Many of these individuals are also constructing arguments based on ideology and theology as a means to promise people external rewards.	140	95	235
Narcissists	These people are using political, foreign policy and individual grievances as a means to whip up a climate of revenge seeking and wanting to fight for the Isis mission and goals.	166	104	270
Identity Seekers	Mostly this is users who appear to be seeking some form of identity. Primarily people searching for some form of masculinity and therefore the Isis recruitment drive appeals to them. This applies to males and females.	87	101	188

Figure 1: Awan, Imran. "Cyber-Extremism: Isis and the Power of Social Media." *SpringerLink*, Humana Press, 15 Mar. 2017, link.springer.com/article/10.1007/s12115-017-0114-0.

I have also decided to use the authors chart to allow the reader to visualize the tools used for ISIS's propaganda:

Table 2 The main tools for propaganda. *recruitment drivers,* type of engagement %

Types	Types of engagement	No of cases
Videos	Extremely dangerous and are used to show online beheadings and online media campaigns.	66
Chatrooms	Using chatrooms or message forums and boards to engage with wider audiences.	21
Websites	The use of visual and written material to depict Isis in a positive light.	12
Images	Use of visual and written communications depicting a 'them vs us' war type mentality and culture. This is also done through the use of leaflets and handbooks.	78
Web links, retweets, likes and hashtags	The use of social media to reaffirm and create normalised behaviour.	96

Figure 2: Awan, Imran. "Cyber-Extremism: Isis and the Power of Social Media." *SpringerLink*, Humana Press, 15 Mar. 2017, link.springer.com/article/10.1007/s12115-017-0114-0.

With these two charts provided, one can group together the behavior characteristics that are susceptible to radicalization and the number radicalized. Secondly, figure 2 allows you to

understand how terrorist recruiters use certain tools for online recruitment. To summarize, the study found that propaganda using videos were the most dangerous and gruesome tactic used for recruitment. The most number of cases found in recruitment tools was web links, retweets, likes and hashtags. The reasoning for this being the most effective is that using these tools kept ISIS's strategies and plans active in to the potential fighter's daily life. The consistency of seeing extremist propaganda created a normalcy to the cause, thus allowing the potential foreign fighter to become more radical. To conclude, these seven characteristics that Awan describes allows me to form a better understanding as to who is willing to sympathize online and why the jihadists recruiting are so successful. Furthermore, knowing these behaviors and types of personalities, it allows for governments to find ways to possibly come up with an effective way of counterterrorism for online recruitment.

Plans for Action and the Obstacles Involved

Christina Archetti in her article *Terrorism, Communication and New Media: Explaining the New Wave of Radicalization* argues that "a greater understanding of communication in the 21st century is essential to more effective counterterrorism in fact, while 'strategic communication' and 'narratives' are advocated by many analysts as essential weapons in countering extremism." (Archetti, 2015, pg. 2)

Christina Archetti explains extremism in a very unique way. She states "The phenomenon of violent extremism takes place in a social world that is constituted by overlapping networks of relationships" (Archetti, 2015, pg. 1). Through "communication technologies" which include apps like Facebook and Facebook messenger, Twitter and WhatsApp take a huge role in forming more direct relationships with the person(s) and extremist group. Through these types of direct and indirect relationships it creates a type of 'imagined community.' thus, this

causes for the person on possibly the opposite side of the world close to the extremist leader and feel a need to live in a Muslim community practicing extremist Islamic law. It is important to note the different narratives Archetti explains that are playing a role in radicalization. There are individual narratives that give us a sense of belonging to our friends, colleagues and teammates. And there is a collective narrative that give us a sense of belonging to societies as a whole. Such as democratic governments, rituals to a religious group. Collective narratives could be used in terrorist organizations as a "mobilization purpose" (Archetti, 2015).

At this point in time one must be thinking what the connection between communication technologies and narratives have in order to cause someone to become radicalized. Well because of these technologies, and the behavioral characteristics discussed, it allows individuals living in completely different parts of the world connect with other like-minded individuals and develop "imagined relationships with people he or she might have never met. In this sense, it is interesting to note that this individual actors, often referred to as "lone wolf," is not alone at all in his/her mind." (Archetti, 2015)

Christina Archetti believes that the most effective tools for counterterrorism is that with "a single local context, through community-based approaches and long-term engagement, it is possible to gain an insight into the local narratives and the networks such narratives arise from." (Archetti, 2015) In other words, one cannot message radical Islamist and try to convince them to change their minds, but if the entire network is contacted the extremist could potentially change his or her "identity" (Archetti, 2015) or way of life. The ultimate goal would be to change the extremist's network and that would lead to de-radicalizing. Although very interesting and compelling article Archetti doesn't provide details as to how a government could go about

'messaging the network' to de-radicalize especially if the individual is so far involved in committed to 'lone wolf' missions.

To bridge the gap between Archetti's article and Awan's is that with Archetti's unique way of explaining the way terrorist recruiters work online and how sympathizer's minds work along with Awan's seven specific key characteristics allows me and the reader to formulate a better understanding as to why online radicalization has worked so well with ISIS. Lastly, with the following policy report it will tie together all of the pieces to formulate the argument as to why governments, specifically the United States government need to evolve their way of countering online terrorism.

The Policy report I examine provides more insight as to how a government could use the internet to counter radicalize. Although written in Great Britain, The International Centre for the Study of Radicalization and Political Violence formulates a variety of interesting and probable ways to combat radicalization. The Scholarship used is crucial to understand why social media and other internet messaging platforms have become such a popular hunting ground for terrorist recruiters. Unfortunately, it is also very difficult to find policy reports that are free to use and therefore I was limited to very few and the report by The International Centre for the Study of Radicalization and Political Violence was the most reliable.

The policy report I will be examining is International Centre for the Study of Radicalization and Political Violence *Countering Online Radicalization: A Strategy for Action (2009)* written by Tim Stevens and Dr. Peter R. Neumann. The focus of this report is to prove that any government organization that aims solely to remove or block extremist material will result unsuccessful. A strategy that aims to reduce the number extremist material and prevent further online radicalization must combine the technical, by making it more difficult to access,

and to make the material itself less desirable. I argue that this way of countering online radicalization would be incredibly affective and believe the United States should use similar methods proposed in the report. I will go into further detail in my case study as to what the United States has done to attempt to counteract online radicalization. However, The U.S has yet to find an effective solution. Overall, I found this report very helpful in my research and a crucial starting point in finding counter strategies for online radicalization.

The report's aim is to develop concrete proposals from within four categories: Deterring producers, Empowering online communities, Reducing the Appeal, Promoting positive messages. Before I begin I would like to acknowledge that this report was published in 2009 and may seem slightly outdated. However, I believe examining reports before the peak of ISIL's perfection on online recruitment serves as a base to examine future policy reports. In the previous two scholarly articles reviewed above, some of following proposals could still be used today. Before I continue with the explanations of the proposals I would like to go into further detail as to why the report argues against using only negative measures/ technical options which results as an ineffective way to counter online radicalization.

The report describes three categories: Removing content from the internet, filtering access to information, and hiding. Removing a website is actually quite straightforward for a government to do. Websites rely on two types of services; The first is a 'domain name provider' aka the URL. And the second is a 'hosting company' that provides the online storage for the URL. In order for the government to remove the website it instructs the host company to take it down. Unfortunately, for this method to work the service provider itself has to be within the same jurisdiction as the government wanting to remove it. For example, if Great Britain wanted to remove a website but discovers the service provider is in Iraq it can't take down the website.

With this said, even if the website operator is within the jurisdiction it can easily move the site to other service providers outside the jurisdiction.

Filtering controls are the information released between computers that are connected with internet. There are a few different types of filters that can be used to block blacklisted IP addresses. Content filtering for example distinguishes key terms that are blacklisted. Although a potentially effective way it is not only incredibly expensive but could also backfire against anti jihadist websites that attempt to red flag the propaganda. With that said, if governments chose to use this method they would also have to come up with some sort of 'whitelist' websites that use those key terms but are non-extremist. This again would result in a very expensive and inefficient method. With many more different categories of filtering the bottom line is that regardless if the government managed to create an inexpensive and efficient way to filter out extremist propaganda. It would still leave out a crucial method to extremist communication, through messaging and private chat rooms.

Hiding is another way of having a certain webpage dropped or made less visible from search engines. A government can so this by interfering with the search engine process and restricting certain extremist webpages. However, this method of combating online radicalization can interfere with certain rights and laws in place to prevent governments from doing such things. Luckily, this method is not really up for debate considering most terrorist propaganda isn't in a web page, it's in social media. Making it even more difficult to filter, remove or even hide the propaganda. To summarize, using any of these methods although can be temporarily effective they are not a long term solution as a strategy for fighting online radicalization. Not only are these methods flawed they could have detrimental effects to a democratic government

that has freedom of speech. In the following paragraphs I will be explaining the four proposals this report offers to combat online radicalization.

The first is proposal is Deterring Producers. In this section of the report, the authors describe that a strategic use of prosecutions along with negative measures can be a positive way to limit and eliminate large parts of online radicalization. Although a good idea this proposal is strictly on British law and finding ways to deter specifically "British based extremists from publishing clearly illegal and/or particularly hateful content." (Stevens & Neumann, 2009, pg. 25) In the second proposal, Empowering online communities, the report emphasizes that the government has a limited ability to overlook the internet and therefore the internet service providers should be doing the policing. From this the internet providers would allow the internet users themselves to regulate the content available.

Empowering online communities proposes an independent internet users panel whose main objective is to strengthen the processes through which internet users can hold internet companies accountable for the content that is published on their platforms. This proposal immediately rose red flags in my head due to the fact that every social media platform has a terms of service upon signing up, which obliges the user to the platforms rules, one of the rules being the prohibition of hateful, extremist content. As argued within this chapter that this method would be exceptionally difficult to combat online extremism due to the "boundaries between what is illegal and what is merely offensive are consequently more difficult to define" (Stevens & Neumann, 2009, pg. 30) and also to find with hundreds of millions of videos, tweets, and statuses uploaded every minute of the day.

Promoting Positive Messages, simply has to do with creating some grassroots start up fund to give money to online initiatives aimed at countering terrorism and extremist messaging

throughout Great Britain. “The aim is to capitalize on the enthusiasm and goodwill of communities around the country who might be willing to invest time and commitment but need limited financial support in order to get their ideas on the net.” (Stevens & Neumann,2009, pg. 43) Not only would this not work in the United States, I have a very difficult time thinking that it would work in Great Britain. I argue that this could lead to an increase in racism. This could be as simple as questioning of every Muslim simply reading the Quran online to harassment on the street or even in local mosques.

Lastly, Reducing the Appeal focuses on how strengthening media literacy especially on impressionable minds is crucial to fighting online radicalization. The report argues that schools play a crucial role in educating children’s minds on online extremism. Specifically, between ages 11-14 where in schools within democratic government are taught the skills for critical understanding and determining what is fact and what is simply an opinion. These would be the crucial ages to have students practice what are signs and clear red flags to an extremist video, image, or webpage. In addition to this argument, since this thesis focuses on Islamic extremist recruitment, I would add that it is also important children ages 11-16 should learn about a brief history of Islam and that most Muslims are not extremist and they are also being attacked by jihadist groups. I think it is crucial that education, both in schools and within the family, is one of the most important factors in red flagging online radicalization and as well decreasing discrimination against the rest of the Muslim community.

International Centre for the Study of Radicalization and Political Violence *Countering Online Radicalization: A Strategy for Action (2009)* written by Tim Stevens and Dr. Peter R. Neumann was a crucial starting point to examine the multiple ways to counter online radicalization. Although this policy report was written in the perspective for Great Britain, these

proposals were also meant for democratic governments like the United States. Lastly, despite the publishing date being 2009, these methods are actually being implemented in the articles talked about above. Such as Archetti's article and how in order to combat online extremism it is crucial to attack the network the extremist is in verses the extremist itself. To an extent, this method is a way of reducing the appeal. It is important to keep these articles and policy report in mind when reading the case study as I discuss the counter terrorism and counter radicalization policies implemented by the Bush and Obama Administrations.

Obstacles are often a part of countering terrorism. As terrorists made the transition to social media, public pressure exploded. As Jessica Stern and J.M Berger explain in their book A State of Terror, social media platforms quickly discovered the difficulties in terrorist propaganda and the actions needed to stop them. YouTube and Facebook were among the first social media platforms to discover those frustrations. The fundamental issue was that suspension of terrorist accounts were predominantly an intelligence issue, however terrorist content on social media was bad for business first, a cultural issue second and national security, third. The reason for this was that "social media is run by for-profit companies, which are neither government services nor philanthropic endeavors" (Stern & Berger, 2015, pg. 139). With this said, the CEO's of the social media companies made the majority of the decisions regarding what to do with terrorist propaganda. Thus, government intervention represented a small part of overall activity (Stern & Berger, 2015). The social media companies had little to no motivation to create limitations for terrorist users who violate the terms of service, nor were the companies inclined to have their users be a resource for reporting terrorist activity.

Facebook became proactive in combatting the propaganda. They shutdown pages, groups, and users. Jihadists noticed this, and found a way to get around it. Jihadists set up

private, members-only Facebook groups to discuss bomb-making formulas and potential terrorist targets, but "blatant plotting soon became a sure ticket to swift and repeated suspensions" (Stern & Berger, 2015, pg. 139). YouTube eventually followed Facebook's lead and lastly so did Twitter. In most cases for government and counter terrorism officials, social media was most useful as a vast hunting ground for investigations and evidence gathering. Specifically, in the United States, the government at times would ask social media companies to keep a certain terrorist users account open in order for the intelligence officials to gather data and potential leads. Meanwhile European countries took to the law by implementing existing hate speech laws into their social media platforms. Middle Eastern countries and South Asia took it one step further in implanting much more aggressive tactics against speech they considered "objectionable" (Stern & Berger, 2015) and many times this objectionable speech was not terrorist related as it was speech opposing the controlling regime.

The United States has been aware of the issue of terrorist recruitment via social media for some time. Unfortunately, as will be further explained in my case study, the United States has not been able to pin point an effective tactic to combat both ISIS and other extremist propaganda on social media while conforming to the needs and desires of the companies that own the social media platforms.

Case Study: Al Qaeda, The Islamic State, and The United States' Counterterrorism Tactics

Al Qaeda and ISIS are world renowned terrorist organizations. However, not many know that ISIS was once an affiliate of Al Qaeda. Currently, Al Qaeda wants nothing to do with ISIL because they are "so brutal and out of control" (Stern & Berger, 2015). In my case study, I have divided this section into three parts: Al Qaeda and the Formation of ISIL, The Generation Gap

between Al-Qaeda and ISIL, and What the United States has done to Counter Terrorism (Al Qaeda & ISIS) from Post 9/11 to the Obama Administration. Within those three parts I divided them into subsections. Part one is Al Qaeda: A Brief History, The Islamic State as an Al Qaeda Affiliate (AQI), The Formation of the Islamic State. Part Two consists of Differences in Attacks, Enemies, Recruitment and Propaganda. Lastly, part three has a subsection on the counterterrorism and counter radicalization tactics implemented during the Bush Administration and the Obama Administration.

Part 1: Al Qaeda and the Formation of ISIL

Al Qaeda: Brief history

Al Qaeda "Emerged out of the anti-Soviet jihad in Afghanistan in the 1980s. As the Soviets prepared to withdraw, Osama bin Laden and a few of his close associates- high on their perceived victory over the mighty Soviet Union- decided to capitalize on the network they had built to take jihad globally. Bin Laden's goal was to "bring under a single umbrella the hundreds of small jihadist groups struggling, often feebly, against their regimes." (Byman & Williams, 2015, pg. 4) Al Qaeda's main target was the United States, not repressive regimes in the Muslim world. This was a different agenda for a jihadist group. Once pledged as a member a jihadi was given access to money, arms, support and the most important, training. Al Qaeda's training camps "were the ivy league of jihadist education." (Stern & Berger, 2015).

The Islamic State as an Al Qaeda affiliate (AQI)

The Islamic State began as an Al Qaeda Affiliate and was among the multiple jihadist groups that formed as a result of the 2003 U.S invasion of Iraq (Byman & Williams, 2015). In 2004 Abu Musab al-Zarqawi (now known as solely Zarqawi), an Al Qaeda affiliate formed a group called Al Qaeda in Iraq (AQI). There were critical fundamental differences between AQI

and Al Qaeda leadership. While Bin Laden was on the run, he still pushed for U.S targets while Zarqawi, and his predecessors after his death in 2006 by a U.S air strike, aimed for more sectarian violence on Sunni Muslims. AQI was also known for its public brutality with horrific beheading videos [ISIL still uses this tactic]. Despite the disapproval from the leadership, Zarqawi's brutal way of war worked well for several years. After the backlash of the indiscriminate violence toward the Iraqi Sunnis, the drastic increase in U.S presence, and a change in strategy in Iraq; AQI was tarnished, and Al Qaeda severed ties with them.

The formation of the Islamic State

In 2010 Abu Bakr Al-Baghdadi took leadership of AQI and when the Syrian Civil War broke out a year later, he urged jihadists to take part of the conflict in hopes of gaining a physical state in the midst of all the chaos. They Succeeded, by 2013 the Iraqi jihadists formally known as Al Qaeda in Iraq called themselves The Islamic State of Iraq and Syria, ISIS. ISIS flourished in Syria because the Syrian regime led by President Bashar Al-Assad, were focused on more moderate rebellion groups. Meanwhile, Nuri al-Maliki, the Iraqi prime minister, put in place a set of disastrous policies to win over Iraqi Shia, which in turn isolated Iraqi Sunni. This helped Baghdadi gain support in Iraq and thus regain legitimacy. By 2014 ISIS swept across Iraq, capturing major cities like Mosul and Tikrit, major hydroelectric dams and oil refineries, as well as multiple border crossings with Syria. With his success, Baghdadi declared himself caliph and "leader of Muslims everywhere" (Stern & Berger, 2015), thus overshadowed Al Qaeda as the forefront of the jihadist war on the west.

Part 2: The Generation Gap between Al Qaeda and ISIS

The competition between Al Qaeda and ISIS is more than just a fight for the more powerful jihadist movement. "The two organizations differ fundamentally on whom they see as

their main enemy, which strategies and tactics to use in attacking that enemy, and which social issues and other concerns to emphasize" (Stern & Berger, 2015). In a later section, I will go into further detail about how the United States has put most of its efforts to counter terrorism on the physical threats to the United States soil and not an effective tactic for cyber-security. For now, I will be focusing on the three critical differences between Al Qaeda and ISIS to help give the reader a better understanding as to why ISIS has changed the way terrorist organization groups operate.

Differences in Enemies

Al Qaeda's ultimate enemy is the United States because they believe they are the primary cause for all of the issues in the Middle East. Their goal is to overthrow the corrupt "apostate regimes in the Middle East and replace them with the true Islamic governments." (Byman & Williams, 2015, pg. 7) They have a "far enemy strategy" which is based on the concept that the U.S military and economic support for Middle East dictators, such as Egypt and Saudi Arabia, which has enabled those regimes to withstand attempts by the jihadists and overthrow them. By attacking the United States, Al Qaeda believes the U.S will withdraw the support of the regimes and pull out of the region altogether, giving the jihadists the opportunity to attack from within. Al Qaeda, in general, does not care about the sectarian divides of Sunni and Shia. They need the support of the Muslim masses, and by attacking Shia Muslims, it is "detrimental to the broader jihadist project." (Byman & Williams, 2015, pg. 8)

ISIS, on the other hand, does not believe in the "far enemy strategy," they have a more "near enemy strategy" which focusses more on the regional level. Their enemy is more the Assad regime in Syria and the Abadi regime in Iraq. ISIS believes they must first "purify" the Islamic community by attacking Shia Muslims and other religious minority communities. Lastly, Al

Qaeda believes in playing nice with others; the Islamic State does not. An example would be Jabhat al- Nusra, an Al Qaeda affiliate in Syria released UN Peacekeepers they had previously captured. Al-Nusra had also worked with Syrian fighters, and instead of terrorizing Syrians to convert to "true" Islam they convinced them. When the U.S launched an attack on Jabhat al-Nusra, many Syrians were frustrated and angry at American because they struck down a "foe of the Assad Regime." (Byman & Williams, 2015) The key for Al Qaeda is to gain allies and allow the military works of the U.S to fuel for hatred and anger.

Differences in Attacks

To fight the United States, Al Qaeda has used terrorism plots known as "spectaculars" (Byman & Williams, 2015). These plots are a way to electrify the Muslim world and to scare off the United States from Muslim territories. They also support insurgencies that fight against U.S backed regimes. Lastly, Al Qaeda has issued a vast amount of propaganda to convince Muslims that jihad is a part of an obligation as a Muslim.

Although ISIL has similar ideals, they approach their tactics differently. ISIS's primary goal is to build a physical Islamic State that could be geographically located. With this said, it's strategy is to control land and expand. By establishing an Islamic State, in their minds, would excite Muslims and attract them to build an army and thus take more land. The only time Al Qaeda has shown interest in controlling territory is for safe havens and a place to train.

Al Qaeda favors large-scale, dramatic attacks against strategic or symbolic targets. The most obvious and famous examples were the attacks on the World Trade Center in New York and the Pentagon in Washington D.C on September 11, 2001.The World Trade Center symbolized the United States' obsession with its capitalist economy and how Americans had no

time or care for God. The Pentagon was targeted due to the military support and physical presence in Saudi Arabia. ISIL, on the other hand, uses social media to express their desires. They want recruits to use whatever is that their disposal to kill as many 'infidels' as possible this has included: running over people with cars or trucks, homemade suicide bombs or conventional bombs. The most elaborately planned attack thus far from ISIS was the attack in Paris on November 13, 2015, during a soccer game, and shooting in a café. ISIS's motive was to inflict fear on a Westerners daily life. ISIS wanted to make sure that the 'infidels' reconsider their secular way of life by drinking coffee and going to a soccer game.

Differences in Recruitment

The purpose for recruitment for Al Qaeda is to draw membership from angry Muslims who were frustrated with the United States Support for Israel or the U.S invasions and interventions in the Muslim world. Post 9/11, Al Qaeda's recruitment growth stemmed from trying to absorb regional jihadists start-ups and convince them that their "struggle is a component of Al Qaeda's sweeping international agenda" (Byman, 2010, pg. 1). Formally joining the organization is complex and usually takes months to years to officially take part. A reason for this is due to the fact that Al Qaeda does not demand sole allegiance like ISIS does. Al Qaeda allows for members to fight for their local/ regional organizations as well as pursuing attacks in the United States and its allies. During this process of fighting against two targets, many members sometimes seek to stay the course of continuing to fight the local regime and others are more attracted to global entities (Byman, 2010). Therefore, Al Qaeda does not offer the open invitation like ISIS does on social media and beyond. Al Qaeda has created significant obstacles for potential fighters, from difficulty of finding the geographic location as to where they are, to

intense religious training that preceded battle (Stern & Berger, 2015). ISIS, believes in a much more open invitation, seeking anyone to fight for them, from those who are rebels fighting the Syrian regime to men and women scrolling through social media looking to fight for a fundamentalist world.

Differences in Propaganda

ISIS's Propaganda in comparison to Al Qaeda's are completely different, Al Qaeda was not formed surrounding the rise of social media, nor even the internet. At Al Qaeda's peak, right after 9/11, Laptops built with Wife and Myspace were the two technological booms of the time. However, ISIS came into power when smartphones and viral videos on YouTube were on the rise. With that said, ISIS's "meteoric rise and its ability to attract tens of thousands of young men (and a few women) to its ranks from around the world, including from many Western countries, its ability to use social media to disseminate its propaganda to its target demographic: angsty Muslim males roughly between the ages of eighteen and thirty-five… the leaders and members of the Islamic State are a generation younger than those of Al Qaeda." (Byman & Williams, 2015) By the summer of 2016, ISIS was reportedly sending 5,000 messages per month via Twitter, Instagram, and other social media outlets to over a billion potential readers. This generation gap especially shows regarding propaganda. Al Qaeda has and continues to rely heavily on older internet platforms such as websites and online forums rather than social media platforms like Facebook and Twitter.

Although Al Qaeda has attempted to update their efforts to keep up with ISIS, they have still only produced the repetitive content with the decade-long footage of Qur'an recitations and pontificating about various aspects of jihad. Meanwhile, ISIS released a series of videos called

Flames of War that show dramatic explosions; clips of Barack Obama and George Bush's bodies CGI'ed on fire; footage of jihadists firing RPG's; graphic, bloody images of executed foes. As stated in my methods and limitations section, I did not purposely search for these brutal videos as the result would lead to a computer virus or a complete shutdown of my computer, however ISIS has previously managed to leak the brutal videos on ordinary people's timelines on Facebook and Twitter, thus making it very easy to come across a video accidentally.

The physical momentum of the Islamic State has drastically diminished with the recapturing of central Iraqi cities such as Mosul. However, they still have a prominent role and dangerous presence in the internet. A recent example would be on December 10, 2018, an Ohio man Damon Joseph, was arrested for allegedly planning to attack a synagogue on behalf of ISIS. United States attorney Justin Herdman stated, "this man spent months planning a violent terrorist attack on behalf of ISIS here in the United States, and eventually targeted a Jewish Synagogue in the Toledo, Ohio area." Joseph was charged on December 10, 2018 with one count of attempting to provide material support to ISIS. Federal agents said that Joseph who was also known as "Abdullah Ali Yusuf" drew their attention to him earlier this year for posting his support of Islamic terrorists on social media accounts, including images that originated from ISIS propaganda.

With this said, counterterrorism strategies used against Al Qaeda cannot be the same with fighting ISIS. Although Joseph is solely one example out of the millions of people using social media in the United States, his arrest proves that with ISIS's domination of propaganda in social media, it was very easy for Joseph, who most likely fell into one of the behavioral characteristics susceptible for radicalization, to find the already released propaganda while ISIS is in hiding from their defeats in geographically located territories. The section on United

States counter-terrorism strategies will go into further detail as to why the tactics being used now are not enough.

The threat is not that ISIS is coming specifically for the United States, the danger is that with ISIS's successful use of social media they have recruited people from within the United States and other western countries to wage war in their name. The simplicity of being able to recruit and manipulate young minds through the power of the internet has not been properly assessed by the United States Defense Department or the United States National Security Agency. The United States tend to look toward a more substantial more prominent physical threat in order to eliminate the most powerful target. However, as explained in my historical analysis, this tactic worked for fighting Al Qaeda and eliminating Osama Bin Laden. However, ISIS's tactics changed that strategy, and it is fundamental that the United States incorporate an efficient way to counter ISIL's virtual powerhouse.

Part 3: What the United States has done to Counter Terrorism (Al Qaeda & ISIS) from Post 9/11 to the Obama Administration

ISIS's articulated strategy for propaganda and recruitment and the simplicity of being able to manipulate young minds through the power of the internet has not been adequately assessed by The United States Defense Department and Department of Homeland Security. The United States has historically looked toward a more substantial more prominent physical threat. The United States aims to kill the organization by its head, literally. Osama Bin Laden's assassination proved to be the greatest victory for the United States on fighting the war on Al Qaeda. This assassination severely weakened Al Qaeda and boosted the United States' morale on the war on terror. Unfortunately, ISIS has forced the United States and other nations to rethink the strategies of counterterrorism, and The United States continues to attempt to eradicate ISIS's

presence online but has proven to be a much more difficult task. Below I will discuss the Counterterrorism policies used under The Bush Administration right after 9/11 and also The Obama Administration Counterterrorism policies during the rise of ISIS. Within each section the subsections are divided into two parts: Counterterrorism policies and Counter Radicalization polices under each administration. Counterterrorism policies are the policies implanted at the time to prevent another terrorist attack similar or potentially worse than the September 11 attacks. Counter-Radicalization policies are tactics implemented to prevent terrorist recruitment from within the United States and abroad.

The Bush Administration and Al Qaeda:

Counterterrorism policies under Bush:

First, the United States went on the offensive, striking back at the 9/11 perpetrators and those who had protected them. The immediate aims were to capture or kill the enemy, expel terrorists from Afghanistan and other geographic safe havens, and ultimately dismantle the global al Qaeda network (Gresson, 2017). In other words, Bush decided to put boots on the ground which led to the U.S invasion of Iraq and Afghanistan, a now 17-year-long gruesome war.

Second, the strategy called for tightening homeland security and improving the counterterrorism capabilities of the country's intelligence and law-enforcement agencies. Bush incorporated the TSA into Homeland Security to increase the safety and security in all national airports. The number of U.S marshals (police that board flights) increased dramatically.

Third, the government ramped up intelligence collection and law enforcement efforts aimed at detecting terrorist plots before they came to fruition. This third policy includes the USA

Patriot Act implemented in 2001 that gave the FBI new investigative tools to prevent a terrorist attack. This included a no-fly list that initially consisted of 16 persons in 2001 to 81,000 today. This policy also created the famous slogan "see something, say something" which as a fellow New Yorker prompts those to be vigilant and possibly prevent an attack from happening by reporting suspicious activity.

Fourth, the United States launched a vigorous effort to cut off funding to terrorist groups. FBI was put in charge of identifying and prosecuting terrorist financiers. The Department of Treasury prioritized that financial institutions collected information on and reported suspicious depositors. Finally, because money flows smoothly across national borders, the United States expanded cross-border intelligence by following financial transactions (Gresson, 2017).

Counter-Radicalization Policies under Bush:

President Bush wanted to diminish the harsh anti-American ideology spreading throughout the Arab world. Bush claimed that "the terrorists were motivated by malice toward American values and the Muslim world was indifferent to their crimes because of a fundamental misunderstanding of America, its society, and values." (Gresson, 2017) What was done was to increase American ideology onto Arab radio waves to potentially debunk the ideologies spread by the extremists and anti-Americans. That was not enough to counter the ideology of the extremists.

Undersecretary of Defense for Policy Douglas Feith said that if U.S. strategy was limited to "protecting the homeland and attacking and disrupting terrorist networks, you're on a treadmill that is likely to get faster and faster with time" and the key to winning the war on terror was "addressing the ideological part of the war that deals with how the terrorists recruit and

indoctrinate new terrorists." (Schmitt & Shanker, 2005, pg. 12) Lastly, in 2006 Jim Glassman was appointed the new Undersecretary of State for Public Diplomacy and Public Affairs. His ultimate goal was to discredit terrorist narratives. He told an audience at the New America Foundation, "our core task in 2008 is to create an environment hostile to violent extremism. We do that in two ways: by undermining extremist ideologies and by encouraging young people to follow productive paths that lead away from terrorism." (Glassman, 2008, pg. 3) Glassman's approach started right as social media began to take off. He wanted to use social media to "portray the image of a society [The United States] that grapples with tough issues, lets millions of voices be heard, and believes that, in the end, the best ideas win." (Glassman, 2008, pg. 3) Glassman predicted that the potential for the internet could be a crucial way to stop terrorism but to also fuel it. Due to the entrance of the new administration, Glassman was unable to continue his approaches.

The Obama Administration:

Under the Obama Administration, President Obama was met with the new challenge of homegrown terrorism intensified through social media and other new communications technologies.

Counterterrorism Policies under Obama:

Obama prioritized the use of drones and special operations forces to fight Al Qaeda while simultaneously removing troops from Iraq and Afghanistan. President Obama succeeded in fighting off Al Qaeda with the assassination of Osama Bin Laden and other Al Qaeda leaders the Administration, however, he was unable to stop the rise of the Islamic State (ISIL). To counter this emerging threat, Obama called for the United States to change their counterterrorism strategy away from large-scale, on the ground, military operations, and targeted interventions

and instead focused more on joining partnerships with nations where terrorist networks were an important issue (Obama, 2014).

Obama's priority was to bring home all U.S troops from Iraq. Unfortunately, things changed when ISIS's footprint increased in Iraq. Obama sent over an additional 5,700 troops to Iraq and trained Iraqi military to fight ISIS. Secondly, Obama expanded the drone program to prevent boots on the ground and fight terrorism from the air. Although a much safer option for Americans, it increased civilian casualties in the region. This gave ISIS more material for propaganda videos because it created fear and anger for America's drones making civilians wanting to fight back. As mentioned before the Arab Spring, which occurred during the Obama Administration, established a fighting ground for ISIS and they took large portions of Iraq and Syria.

In August of 2014 ISIL filmed the beheadings of American journalists James Foley and Steven Sotloff. The 'anti-ISIS' campaign would ultimately expand to include military advisers, Special Operations Forces, and other American employees partnering with local allies on the ground, keeping its footprint limited while enhancing the operational effectiveness of the Iraqi military, Kurdish Peshmerga militias, and other local partners/militia (Gresson 2017). By 2017, ISIS had lost substantial parts of their 'Islamic State.' However, homegrown terrorism was becoming a significant issue. From the Boston Marathon bombings in 2013 to the San Bernardino shootings in 2015 and the Orlando shooting in 2016. All had extremist Islamic beliefs, and many swore allegiance to ISIS.

Counter-Radicalization policies under Obama:

Social media, maps, and other communication technologies enabled law enforcement to collect volumes of data to target and surveil potential terrorist targets. This data alone now informs more than a quarter of the NSA's reports on international terrorism. (Privacy and Civil Liberties Oversight Board, 2008) However, the internet, as you now know through my research and Literature, has proved to be an active recruiting and radicalization tool for terrorist groups, especially ISIS, which by summer 2016 was reportedly sending 5,000 messages per month via Twitter, Instagram, and other social media outlets to over a billion potential readers. While communications were long an operational vulnerability for terrorists, recent advances in commercially available, powerful encryptions have enabled terrorists to hide the content of their contacts from intelligence and law enforcement agencies.

In 2011, Obama's Administration created the Center for Strategic Counterterrorism Communications (CSCC) to focus more on counter-messaging and social media recruitment. The way CSCC did this was that they mounted campaigns across social media platforms. This included producing YouTube videos in multiple languages and establishing a Twitter presence where CSCC staff would go toe-to-toe with terrorist group members and supporters online. (Gresson, 2017) Although tackling online radicalization and those susceptible to falling into the trap of extremist ideology was the ultimate goal, the CSCC had an annual budget (5-6 million a year) that was just not enough to target this vast mission (Miller & Higham, 2015) The CSCC was also greatly outnumbered by the Islamic State and other terrorist organizations, and thus faced a deluge of online recruiting accounts and sites, with not enough resources and capital to successfully counter the dissemination of information and propaganda (Gresson 2017).

The CSCC experimented with different approaches to combat online recruitment. However, the future for CSCC remained bleak. By 2016, CSCC was rebranded and renamed to

the Global Engagement Center (GEC)tasked with four essential tasks: "building partnerships with governments, NGOs, communities, and religious organizations; utilizing data analytics to better target messaging; producing collaborative content to counter the Islamic State; and acting as a liaison for numerous national security agencies operating in the information sphere" (Gresson 2017). The GEC put their focus on promoting and establishing partnerships with foreign governments to assist in the spread of more localized messages (Gresson 2017) and eventually wholly strayed from the direct messaging ideal the CSCC prioritized. Instead, the GEC partnered with local counter-messaging centers such as the UAE's Sawab Center and Malaysia's Regional.

Although President Obama successfully weakened ISIS's physical footprint, it is still likely the terrorist organization will come back. With the help of U.S forces the Iraqi military took back Mosul, and in Syria, the Assad regime seized again Raqqa, which was ISIS's de facto capital. Neither of these two cities is stable. The Iraqis still struggle with ethnic tensions and Syria is decimated from the almost eight-year-long civil war. ISIS also has affiliates in Malaysia and Nigeria that created carnage. Lastly, ISIS has never removed their footprint in cyberspace and can thus recreate their propaganda videos, and continue to message possible recruits from wherever they are hiding.

Analysis

My thesis has argued the dangers of online radicalization and demonstrated the unsuccessful attempts of the United States to counter the phenomenon of ISIS's social media empire. The literature review suggests that there are certain types of personality traits within a person that uses social media and other web messaging platforms that may make them

susceptible to radicalization. These seven characteristics of whom are likely to be sympathizers as well as those recruiting are: cyber mobs, loners, fantasists, thrill seekers, moral crusaders, narcissists, identity seekers. Figure 2 allows you to understand how terrorist recruiters use certain tools for online recruitment. The study found that propaganda using videos were the most dangerous and gruesome tactic used for recruitment. The most number of cases found in recruitment tools was web links, retweets, likes and hashtags. The reasoning for this being the most effective is that using these tools kept ISIS's strategies and plans active in the potential fighter's daily life. The consistency of seeing extremist propaganda created a normalcy to the cause, thus allowing the potential foreign fighter to become more radical. Although evidence suggests that social media as a whole tends to discourage extremism in the general population, for those already vulnerable to radicalization it creates dark pools for social connections that can be found by terrorist recruiters and influencers. On twitter and Facebook, it is easy to seek out or stumble onto a radical or extremist account or community, and even easier for terrorist organizations to seek prey within mainstream society (Stern & Berger, 2015).

Christina Archetti's article reiterates Imran's argument through her definition of "communication technologies." Through "communication technologies," which include apps like Facebook and Facebook messenger, Twitter and WhatsApp, take a huge role in forming more direct relationships with the person(s) and extremist group. Through these types of direct and indirect relationships it creates a type of 'imagined community.' thus, this causes for the person on possibly the opposite side of the world close to the extremist leader and feel a need to live in a Muslim community practicing extremist Islamic law.

The policy report I reviewed provides suggestions for counterterrorism analysts to consider incorporating in the development of new tactics. However, as stated in my case study,

the United States has not incorporated those methods in their counterterrorism tactics. The report's aim is to develop concrete proposals from within four categories: Deterring producers, Empowering online communities, Reducing the Appeal, Promoting positive messages. Deterring Producers, a strategic use of prosecutions along with negative measures can be a positive way to limit and eliminate large parts of online radicalization. As states before, this proposal is focused strictly on British law. Empowering online communities, the report emphasizes that the government has a limited ability to overlook the internet and therefore the internet service providers should be doing the policing. From this, the internet providers would allow the internet users themselves to regulate the content available. Empowering online communities proposes an independent internet users panel whose main objective is to strengthen the processes through which internet users can hold internet companies accountable for the content that is published on their platforms.

This proposal immediately rose red flags in my head due to the fact that every social media platform has a terms of service upon signing up, which obliges the user to the platforms rules, one of the rules being the prohibition of hateful, extremist content. However, terrorist organizations have managed to get around those rules by lack of surveillance and switching to private messenger within the same social media platform. Promoting Positive Messages, simply has to do with creating startup funds to give money to online initiatives aimed at countering terrorism and extremist messaging throughout Great Britain. Lastly, Reducing the Appeal focuses on how strengthening media literacy especially on impressionable minds is crucial to fighting online radicalization. Lastly, the report argues that schools play a crucial role in educating children's minds on online extremism.

To reiterate, social media platforms quickly discovered the difficulties in terrorist

propaganda and the actions needed to stop them. YouTube and Facebook were among the first social media platforms to discover those frustrations. The fundamental issue was that suspension of terrorist accounts were predominantly an intelligence issue, however terrorist content on social media was bad for business first, a cultural issue second and national security, third. This mentality slowed down the process for an effective counter radicalization and terrorism strategy that could have significantly weakened ISIS's virtual footprint.

The United States continues to fight the same war on terror but with advanced technology. The predominant difference is the missions that were done on foot with military personnel are now done with drones. It is true that the United States has significantly weakened ISIS's physical footprint in both Iraq and Syria. However, ISIS continues to be present online and unless the United States finds a way to weaken and eliminate ISIS's virtual footprint, the future of cyber security will be in jeopardy. ISIS has forced nations across the globe to reinvent the way terrorism should be dealt with. I would argue the way to fight online radicalization is to put oneself in the mind of the recruiter and the potential foreign fighter. It is important to analyze the behavioral characteristics that may fall into extremism and to also know and understand why certain internet tools are used more than others. Lastly, it is vital to understand that Al Qaeda and ISIS although once affiliated are two very different organizations with different goals in mind. Therefore, the strategies of attack should not be the same.

Conclusion

Throughout this thesis I argued the dangers of online radicalization, explained how ISIS was able to develop and perfect their online propaganda by attracting thousands of vulnerable young adolescents to fight for their cause. I demonstrated the psychology behind online

radicalization and the behavioral characteristics that are susceptible to radicalization. In the case study presented, I compared Al Qaeda's role and their weaknesses in propaganda compared to ISIS' and then provided the multitude of counter terrorist and radicalization policies used under the Bush and Obama Administrations. As a result, it was evident that The United States has been successful in severely weakening both Al Qaeda's and ISIS's physical footprint in the Middle East but have been unsuccessful, on multiple attempts, to weaken ISIS's virtual footprint. Therefore, with the unsuccessful attempts to weaken ISIS' online presence it will be exponentially difficult when a more technologically advanced terrorist organization appears.

Lastly, it is important to discuss the lingering questions a reader may have. This thesis concludes that ISIS has become the terrorist organization with the most recruits through social media and other direct internet messaging. With ISIS's highly advanced technological recruitment tactics, it has been exceptionally difficult for nations like the United States to react and weaken ISIS' virtual footprint. This thesis has not been able to pinpoint a solution to how to counter ISIS' propaganda but has offered multiple insights on the different angles a nation can work with to fight online radicalization.

Bibliography:

Archetti, C. (n.d.). Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/401/html

Awan, I. "Cyber-Extremism: Isis and the Power of Social Media." *SpringerLink*, Humana Press, 15 Mar. 2017, link.springer.com/article/10.1007/s12115-017-0114-0.

Byman, D. L. (2016, July 28). Al Qaeda's M&A Strategy. Retrieved from https://www.brookings.edu/opinions/al-qaedas-ma-strategy/#cancel

Byman, D. L., & Williams, J. R. (2015, February 24). ISIS vs. Al Qaeda: Jihadism's global civil war. Retrieved from https://www.brookings.edu/articles/isis-vs-al-qaeda-jihadisms-global-civil-war/

Engel, P. (2015, May 09). ISIS has mastered a crucial recruiting tactic no terrorist group has ever conquered. Retrieved from https://www.businessinsider.com/isis-is-revolutionizing-international-terrorism-2015-5

Gresson, R. (2018, September 06). Defeating Terrorists, Not Terrorism: Assessing U.S. Counterterrorism Policy from 9/11 to ISIS. Retrieved from https://bipartisanpolicy.org/library/counterterrorism-policy-from-911-to-isis/

Glassman J.K. *"Public Diplomacy 2.0: A New Approach to Global Engagement."* Remarks at The New America Foundation. December 1, 2008.

Korte, G. (2018, December 11). FBI: Ohio man arrested in Toledo synagogue plot, said he was inspired by Pittsburgh shooting. Retrieved from https://www.usatoday.com/story/news/nation/2018/12/10/damon-joseph-toledo-synagogue-shooting-isis-pittsburgh-robert-bowers-fbi/2269765002/

Miller G. and Higham S. *"In A Propaganda War Against ISIS, The U.S. Tried to Play by the Enemy's Rules."* The Washington Post. May 8, 2015

Privacy and Civil Liberties Oversight Board. *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.* July 2, 2014. 108.

Schmitt E. and Shanker T. *"U.S. Officials Retool Slogan for Terror War."* The New York Times. July 26, 2005.

Stern, J. S., & Berger, J. M. (2016). *ISIS: The State of Terror*. Harper Collins UK.

Stevens, T. and Neumann P.R. *Countering Online Radicalization*. 2009, cst.org.uk/docs/countering_online_radicalisation1.pdf.

Project, C. (2018, February 28). Al-Qaeda Recruitment Methods Revealed. Retrieved from https://clarionproject.org/al-qaeda-recruitment-methods-revealed/

Remarks by the President at the United States Military Academy Commencement Ceremony. May 28, 2014.