REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
	MMS	

4. TITLE AND SUBTITLE

#Jihad: Establishing an Effective US Strategy to Combat Terror Online

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
LCDR W.A. Shafer

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
United States Marine Corps
Command and Staff College
Marine Corps University
Quantico, Virginia 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper highlights the failure of the United States to develop an effective strategy to successfully counter and disrupt extremist use of social media as a pathway to recruit, radicalize, and conduct attack planning, and then provides a basic interim military strategy that can fill the gap until a broader, viable United States government and international policy can be established that effectively disrupts extremist use of social media.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	56	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
#Jihad: Establishing an Effective US Strategy to Combat Terror Online

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:
LCDR W.A. Shafer

AY 15-16

Mentor and Oral Defense Committee Member: MATTHEW FLYNN
Approved: ✓
Date: 2/1/16

Oral Defense Committee Member: Robert S. Peterson
Approved: ✓
Date: 2/1/16

Approved
2/1/16

Executive Summary

Title: #Jihad: Establishing an Effective US Strategy to Combat Terror Online

Author: Lieutenant Commander William Anthony Shafer, United States Navy

Thesis: This paper highlights the failure of the United States to develop an effective strategy to successfully counter and disrupt extremist use of social media as a pathway to recruit, radicalize, and conduct attack planning, and then provides a basic interim military strategy that can fill the gap until a broader, viable United States government and international policy can be established that effectively disrupts extremist use of social media.

Discussion: Over the last 15 years, terror groups have advanced their use of online technology to enable their operations and spread ideologies. Specifically, terror groups exploit the Internet and social media platforms to gain support, recruit and radicalize new members, and inspire lone wolf attacks throughout the world. Use of social media provides extremist groups the ability to reach new audiences and extend reach across international borders to sympathizers' cell phones and computers with relative ease. These groups continue to utilize and capitalize on emerging technologies and applications faster than the technology can be countered. The US and its various international partners do have an active strategy to counter extremist use of social media. However, that strategy has proven ineffective. The US government does recognize the use of social media as a significant problem in the fight against terrorism but lacks a strategy to impact groups like ISIS. The United States is in the process of refining its domestic strategy to combat terrorism as well as broadening its international coalition; however, while these coalitions mature, the US military can be leveraged to better counter terror groups online. This study examines terrorist use of social media, what they gain from it, and proposes a strategy that will be more effective in combating extremist use of the Internet and social media.

Conclusion: The US strategy needs to give legitimacy to combating terrorist groups online that equals that of all other components of the overarching strategy. The US must broaden its international partnership, specifically with Muslim countries, to further the legitimacy of the fight to combat radical Islamic ideology. The strategy also needs to expand the role of the US military that has the capability and capacity to conduct operations to counter terrorist groups. With expanded authorities, the US military can quickly impact terror groups like ISIS in order to disrupt their operations in the cyber realm.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Page

Preface

Combating terrorism is a challenging mission. In recent years counter terrorism has expanded from the battlefields of Afghanistan and Iraq and safe havens like Yemen and Somalia to the cyber world of laptops and smart phones. The Internet and social media platforms have expanded the reach of terror groups and have allowed them the ability to cross international boundaries with a click of a mouse. Terror groups continue to outpace the United States and its international partners with their sophisticated use of media and social media platforms to enable their operations. Technology and the exploitation of technology have made terrorism much harder to combat. The topic of extremist use of social media will become more important in the years to come as the US government determines how it addresses this growing threat. The US military should be doing more to target key online terrorist recruiters, facilitators, and planners. This paper is an attempt to outline what the US military could do while the US inadvertently continues to execute an ineffective counter terrorism strategy.

Professor Matthew J. Flynn's mentorship was critical for the development and refinement of this paper. His guidance and perspective were invaluable in the completion of this study. Credit is also due to those interviewed to gain additional insights. Members of the Department of State and J.M. Berger in particular were key for this paper.

REPORT DOCUMENTATION PAGE

FORM APPROVED - - - OMB NO. 0704-0188

1. AGENCY USE ONLY (*LEAVE BLANK)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED *STUDENT RESEARCH PAPER*
4. TITLE AND SUBTITLE		5. FUNDING NUMBERS i *N/A*
6. AUTHOR(S)		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) *USMC COMMAND AND STAFF COLLEGE* *2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068*		8. PERFORMING ORGANIZATION REPORT NUMBER *NONE*
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) *SAME AS #7.*		10. SPONSORING/MONITORING AGENCY REPORT NUMBER: *NONE*
11. SUPPLEMENTARY NOTES *NONE*		
12A. DISTRIBUTION/AVAILABILITY STATEMENT *NO RESTRICTIONS*		12B. DISTRIBUTION CODE *N/A*
ABSTRACT *(MAXIMUM 200 WORDS)*		
14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH)		15. NUMBER OF PAGES: 16. PRICE CODE: N/A

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE:	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	*UNCLASSIFIED*	*UNCLASSIFIED*	

#JIHAD

Establishing an Effective US Strategy to Combat Terror Online

"It's not that ISIS is so great, it's that the response against ISIS is both limited and weak."
-Alberto Fernandez, former director of the Center for Strategic Counterterrorism Communications (CSCC) [1]

INTRODUCTION

On May 3, 2015, Elton Simpson and Nadir Soofi attacked a crowd gathering at a cartoon-drawling contest in Texas, a forum these two believed was defacing the prophet Mohammad, founder of Islam.[2] The attack ultimately failed after security intercepted and killed the attackers. The attempt could have been prevented altogether if the United States government had a better overall strategy with dealing with extremist use of social media to recruit, radicalize, and conduct attack planning. Prior to the attack in Garland, Texas, Simpson had been in contact via social media with Mohamed Abdullahi Hassan (aka "Miski"), a Minnesota-born, United States citizen and a member of the terrorist organization Al-Shabaab located in Somalia. Hassan was also an active online recruiter for militant Islamic groups.[3] Simpson and Miski shared numerous Twitter exchanges in the days leading to the failed attack both in open Twitter conversations and in closed "secret" discussions on Twitter.[4] It is not fully known what was said between the two in private social media chat rooms, because there is no open source data on the exchange, but it can be assumed the two discussed details on the planned attack in Garland. What is fact is that Miski had provided information on his various social media sites with information on the event in Garland with commentary on the fact that United States-based extremists need to conduct attacks much like the attacks carried out targeting the French newspaper Charlie Hebdo. Miski's Tweets stated, "The brothers from the Charlie Hebdo attack did their part. It's time for the brothers in the #US to do their part."[5]

With the advance of technology and the United States government's ability to monitor communications of known extremists, could the attack in Garland, Texas have been prevented? The answer is yes. The attack could have been prevented at various points along the path to active terrorist, from both domestic and international actors and recruiters. Facilitators of terrorism such as Miski should be targeted, captured, and exploited in order to gain a better understanding of how extremists utilize the Internet to further their cause and gain support. Is the United States government doing enough to stop extremists from using social media outlets to recruit, radicalize, and conduct attack planning online? The answer is no. The United States does not have an effective policy or strategy to combat extremists such as the Islamic State in Iraq and Syria (ISIS will be the acronym used in this paper vice other naming conventions for this terrorist organization) using social media to gain influence online. This study highlights the failure of the United States to develop an effective strategy to successfully counter and disrupt extremist use of social media as a pathway to recruit, radicalize, and conduct attack planning, and then provides a basic military strategy that can fill the gap until a broader, viable United States government policy can be established that does curb extremist use of social media.

There are concerns and protests by privacy activists and organizations about privacy and government's ability to monitor private web accounts and social media. The companies that administer and control accounts (such as Twitter and Facebook) all have differing rules that define when a specific user account has crossed the line into extreme ideology and/or terrorist activity. The US government has battled with these companies in attempt to shut down or to continue monitoring specific accounts. There is currently no

standard defining when a company will work with the United States government and share information on specific accounts suspected of being connected to terrorism operations. After the December 2, 2015 shooting in San Bernardino, there have been increased calls from US government officials for social media companies to do more to fight terrorism.[6] There needs to be a common working relationship between all social media outlets and the United States government on what constitutes extremist operations on social media to ensure that there is a clear standard on when the Internet is being used as a platform for terror. Then, methods to counter this activity can take shape.

This paper is focused on US senior military and political leaders in order to identify the possibility of a policy that will unify various US government departments and organizations to counter extremist use of social media, to engage a whole of government and international partnership approach to counter message terrorist propaganda, and to utilize existing authorities to target individuals who are facilitating recruitment, radicalization, attack preparation, and exploitation of those who wish to join extremist groups and/or want to execute terror attacks.

SOURCES REVIEW

Sources for this paper were gathered from a variety of publications ranging from scholarly books, congressional testimony, and journal articles discussing the rising use of social media by these terror groups; this paper is designed to get past the deluge of newspaper-magazine stories on the topic. The issue of extremist use of social media is an evolving topic that is playing out with each terror or lone wolf attack, as all seem to have a social media aspect to them generally exposed by US media outlets whether true or not. Technology continues to advance making the topic even more fluid as terror groups

rapidly expand their ability to exploit media just as fast as it is introduced on the market. Gabriel Weimann stated in his 2006 book *Terror on the Internet: The New Arena, The New Challenges*, that "terrorism on the Internet is a very dynamic phenomenon: Web sites suddenly emerge, frequently modify their formats, and then swiftly disappear—or, in many cases, seem to disappear but actually have only moved by their changing their online address, while retaining much of the same content."[7] Weimann's statement remains true today as technology continues to rapidly advance and is more accessible and easier to use. Social media is also a relatively new type of communications method that has changed the pace of global communications between people, specifically the use of smart phones as platforms to access the World Wide Web. This fast paced environment makes keeping up and understanding how social media is being exploited by terror groups extremely hard, as to be expected of a contemporary topic.

Books analyzing groups like AQAP and ISIS do illustrate that these groups have progressively advanced the use of social media, but do not address how to combat that use. These sources were great to gain an understanding of how the groups originated and operate, but are poor in regard to developing a strategy to defeat them online. For example, Jay Sekulow's *Rise of ISIS: A Threat We Can't Ignore* provides great insight into the origins and ideology of ISIS but does not generate any narrative on how to better combat them on social media. Specifically, Erick Stakelbeck's *ISIS Exposed* and Jessica Stern and J.M. Berger's book *ISIS: The State of Terror* discuss in-depth how terror groups have evolved their use of media to bolster their recruitment, support, and planning, but fall short of discussing a strategy to better combat them.

Congressional hearings concerning terror groups and national security also provide insight into the growing concern of the US government about increased terrorism and the evolving role social media plays as a weapon of terror. These hearings provide specific insights from Subject Matter Experts (SMEs) on the topic of terror and social media like Peter Bergen, a well-known journalist and author focusing on terrorism, and J.M. Berger, the author mentioned above and nonresident fellow at the Brookings Institution who specializes in social media. Berger, in particular, has led the field in research and analysis of terror groups' usage of social media. He has published books, articles, papers, and has testified before Congress on several occasions to discuss how terror groups use social media and has worked with most of the social media companies to study the amount of data, accounts, re-posts, and followers these groups have online.

In-depth publications covering how to combat groups like ISIS online has not had enough time to fully mature. The majority of documentation on this topic focuses on how the groups use media rather than how to defeat them. These books, articles, and studies do a great job on framing the growing and innovative usage of social media, but fall short in terms of countering it. Primary sourcing for this paper assists in developing a proposed effective strategy to counter terror groups on various media platforms. Interviews were used with a number of SMEs to gain a better perspective, to achieve insights, and to supplement the bibliography for this paper. Interviews conducted for this paper were with J.M. Berger, State Department's Principle Deputy Assistant Secretary (PDAS) Gerald Feierstein, members of the Department of State's Bureau of Counterterrorism, and members of the State Department's Center for Strategic Counterterrorism Communications (CSSC) who are mandated by executive order to counter radical

ideology online. Naval Postgraduate Center for Homeland Defense and Securities Professor Anders Strindberg's perspective on community involvement on counter-radicalization and policing provided a unique contribution to the proposed strategy.

The interviews for this paper had one striking theme, which is there is no clear end state or goal in regard to combating extremism online. Thomas Rodebaugh, the State Department's Director for Digital Outreach in the Center for Strategic Counterterrorism Communications, stated that there is no overarching end state which makes gauging the overall effectiveness of the US's messaging narrative online extremely difficult to judge.[8] This sentiment was shared by all of those interviewed.

With no clearly defined end state to counter terrorist groups online, counter activities become a daily grind of "contesting the space" rather than conducting effective counter-narratives or slowing terror groups' ability to utilize the Internet as a vessel to assist its operations. The CSSC only conducts "fact based" online information exchanges targeting "fence sitters" and does not engage with known extremist members on a routine basis.[9] "Fact based" information does not challenge or engage in discussions about ideology or religion, rather it focuses on discussing events or actions by terror groups and countering it with differing view points on what actually happened. J.M Berger stated that this strategy is not effective and it is time to transition to a more "disruptive" approach in order to create doubt and fear into the online networks.[10] The discussions during these interviews assisted incredibly in framing the current problem of terrorist use of social media and in developing a strategy moving forward to combat it in a more effective manner. However, the interviews were also extremely underwhelming in regard to current US efforts to combat terrorism online. It was very apparent during the

interviews that terrorist use of social media and utilizing the Internet as a weapon is recognized as a problem that must be addressed, but the United States does not take the matter seriously enough to have a plan to do something about it other than "contesting the space." This phrase was a common theme during the interviews at the Department of State and will get more attention in the pages that follow. The phrase "contesting the space" highlights a lack of a needed goal or clear end state to counter terrorist use of social media. This paper hopes to push things in the direction of forming an effective strategy.

BACKGROUND

Social media can take numerous forms today due to the rapid growth of technologies that facilitate user connection to the Internet. YouTube, Twitter, Facebook, LinkedIn, Tumblr, and Instagram are just a few of the social media outlets that allow for the passing of information online. Any of the above and some unlisted outlets may be the vessel that extremists use to initiate contact and communications with those who sympathize with extremist groups and wish to support or join their cause. Social media, which was created to connect people, provides extremist groups like ISIS the ability to spread its message to anyone who has access to the Internet. ISIS's ability to spread its message online can influence those who originally did not desire to support terrorist groups, but found ISIS's ideology online inspiring, or can provide those who already had a desire to support or execute terrorism the ability to have information available that supports their own extreme ideology. The Internet just provided them the needed encouragement and resources to move toward terrorism.

There are numerous publications about the rise of ISIS and the security threat they pose to the United States. Most, if not all, agree that ISIS's use of technology, specifically the Internet and social media outlets, has expanded in their sophistication to the point that countries such as the United States cannot keep pace with how ISIS utilizes social media, and how it avoids being shut down by utilizing procedures that allows them to change account names or create new accounts before they are suspended by social media companies.[11] Representative John Ratcliffe, Republican Congressmen from the 4th District of Texas, remarked during a June 3, 2015 House Committee on Homeland Security hearing that, "Their (ISIS's) sophisticated use of social media has become a terrorism multiplier," and that, "They have become a terror franchise."[12] ISIS users avoid being shut down by various methods like changing online handles and accounts frequently to avoid security organizations from monitoring their accounts for long periods of time.

ISIS also uses trending hash tags of non-extremist activities to get huge numbers of online users to be exposed to extremist propaganda. In 2014, ISIS used #Worldcup2014 to lure people interested in soccer to a hash tag offering updates on the most current ISIS battle in Syria.[13] With frequent account changes and utilizing seemingly innocent hash tags, continuous monitoring of these accounts is almost impossible. Also, social media companies' terms and agreements allow users to press the line on what is and is not "extreme" which gives maneuverable space for extremist groups to express extreme ideology without having their accounts revoked.

During his opening statement at the *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment* hearing before the Senate Committee on Homeland Security and

Governmental Affairs, Democratic Senator Thomas Carper from Delaware made the following remarks: "Groups like ISIS, Al-Shabaab and Al-Qaeda in the Arabian Peninsula have used social media and online propaganda to spread their call to extremists here in America and around the world to carry out their own attacks against."[14] This statement is a very over-simplified example of how long extremist and terrorist organizations have been utilizing social media to spread their ideology, recruit both fighters and supporters, and inspire lone wolf attacks all over the globe.[15] Recent media attention has been mostly focused on ISIS, but Senator Carper's comments also reference Al-Shabaab (based in Somalia[16]) and Al-Qaeda in the Arabian Peninsula (AQAP, based in Yemen[17]) who were recognized terrorist organizations long before the inception of ISIS.

Before AQAP's American born cleric Anwar al-Awlaki was killed by a US drone strike in Yemen, he spread AQAP's ideology using social media to recruit, radicalize, and plan terror attacks focusing on the United States.[18] Using social media outlets such as YouTube, he reached thousands of viewers and spread AQAP's anti-West rhetoric.[19] Social media in this case provided those who had similar anti-West sentiment the access to lecture style videos from a prominent cleric to further their ideology. One individual who received the message was Major Nidal Malik Hasan who conducted the mass shootings at Fort Hood, Texas. Major Hasan and al-Awlaki reportedly exchanged numerous emails prior to the shooting.[20] It can be assumed that Major Hasan viewed al-Awlaki's videos online, and his connection with the ideology and message of Awalki's preaching and rhetoric influenced his actions in Texas.

AQAP had the ability to not only utilize an English speaking radical on social media, it took to publishing its own magazine to further reach the masses. *Inspire* magazine, along with other social media projects, illustrates a more advanced approach to the use of the Internet designed to reach those who were before unreachable. The intent of *Inspire* is to impact English-speaking countries in an attempt to recruit and radicalize future jihadists.[21] *Inspire* magazine continues to be published on a routine basis despite attempts by the United States to stop its publication and distribution online. To date, there have been fourteen issues released, the last issue being September 2015.[22] Dzhokhar Tsarnaev and Tamerlan Tsarnaev constructed pressure cooker bombs to terrorize the Boston Marathon with instruction from *Inspire* Magazine.[23]

AQAP's use of the Internet is just one example of one terrorist organization's use of social media to spread virtual terror. AQAP raised the bar in how they utilized social media, but other groups like Al-Qaeda in Iraq (AQI[24]) under Abu Mus'ab al-Zarqawi was also extremely active on social media to include releasing execution (beheadings) tapes that went viral on various extremist websites.[25] Extremist use of the Internet and social media is not a new concept as history tells us. As technology advances, so does extremists' understanding and sophistication on how they use social media to include their own security procedures. This increased sophistication, from videos posted on YouTube by Anwar al-Awlaki, Al-Shabaab using Twitter to provide real-time updates as it attacked the Westgate mall in Nairobi, and ISIS's Hollywood quality video production and use of Twitter, illustrates that there are no bounds to what these groups can do on the Internet; only their own imaginations can hold them back.

The use of social media by Al-Qaeda (AQ) and its various affiliates did not develop overnight; rather, over a long period of time, AQ had operational ability to refine and advance their skill-set in the cyber world. Allowed this ample time to perfect its online capabilities, AQ has maximized its efforts - which generates questions. Where has the United States been and why has the world's most powerful nation not increased its ability to disrupt or effectively counter extremists' use of social media?

WHAT TERROR GROUPS GAIN FROM USING SOCIAL MEDIA

Social media allows groups like ISIS the ability to gain support for its cause, recruit and radicalize new members, and inspire lone wolf style attacks worldwide to include the United States. Regardless if an individual desires to join ISIS ranks, the mere fact that they are following ISIS media indicates a form of support at the basic level for what ISIS is doing. The "war of ideas," as Dr. Max Abrahms (a political science professor at Northeastern University) refers to the conversation circling ISIS's propaganda machine, will be fought or won at its base foundation.[26] If ISIS can continue to have online followers and expand the number of people who follow their online community at the basic level, then their support will continue to flourish. Regardless if the intent is to actually physically join ISIS and fight, or if those who follow ISIS online have chosen their side in the "war of ideas", there is increased likelihood that these online followers would support ISIS by other means, namely through spreading the ISIS message by sharing the group's social media links, offering financial support, or supporting those in their communities who desire to join ISIS. As long as ISIS can continue to gain support and have an online audience, their ability to continue their fight will continue.

The estimates vary on how many social media messages are sent out daily by ISIS. Several estimates range between 90,000 to 100,000 messages per day, not including the number of people that repost messages on their personal accounts.[27] It is possible that ISIS's messages reach millions of people per day; it is debatable if not impossible to be able to correctly judge if people truly read and digest the ISIS material or merely glance at it or ignore it. J.M. Berger and Jonathon Morgan in their paper, *The ISIS Twitter Census,* analyze the large number of followers online, but illustrate that there are three groups of people - covert supporters of ISIS, pro-ISIS intelligence operatives, and anti-ISIS intelligence operatives. The categories make it hard to judge who is doing what with social media.[28] Regardless, there is the potential for a huge number of people to be exposed to ISIS propaganda each day.

This vast pool of people allows ISIS the ability to focus in on those who are more engaged with the group via social media. ISIS needs to really only focus on a small-identified group of followers who show interest in their cause. With a huge group of followers, there is going to be a percentage of people who want to be more involved and show interest in joining their ranks. The wide net cast by ISIS allows them to get their message out to a large number of people but also to identify who is willing to support them, all through interaction online. This begins the process by which the group can start the recruitment process. Members can be recruited for different reasons based upon what they can do for the organization. ISIS can recruit individuals for their specific skills, areas like finance or computer-based knowledge. Social media is what links those individuals who have a desire to support ISIS either by physically joining them or by providing facilitation and specific skills online.

Online connection also contributes and assists in the execution of lone wolf attacks. ISIS has been credited with inspiring several lone wolf attacks in the United States and other countries in the world. Lone wolf attacks add to ISIS's brand and their ability to spread terror worldwide. Lone wolf attacks have yet to be spectacular aggressions, unlike the attacks on the world trade center on September 11, 2001, but they do generate "spectacular reactions" once completed.[29] Any attack will generate fear. Recent mass shootings in the US have sparked fear in people that while watching a movie they might be caught in a violent assault. However, when an individual conducts a violent attack inspired by groups like ISIS, it generates a different kind of fear - a fear that the wars raging in Syria and Iraq are not really that far away and that there are ISIS members among the masses in America.[30]

So how is this all done over the Internet? J.M. Berger in his article, *Tailored Online Interventions: The Islamic State's Recruitment Strategy*, argues that the terror groups have established a process to vet, assess, and identify those individuals who want to support the group. Mr. Berger breaks the process down into four steps:

1. Contact is initiated by either online ISIS members or by individuals who find or follow ISIS social media.
2. Contact is maintained to allow incorporation of the individual into an online community. This allows ISIS to have constant virtual contact with the individual in order to assess them and encourage further radicalization.
3. Transition is made from open social media to a private communication platform like WhatsApp, Kik, Surespot, or Telegram. At this stage ISIS has identified that the individual has the ability and will to do something for the organization, like

joining the group to fight or to conduct an independent attack. Moving the conversation provides additional security and hinders law enforcement and intelligence organizations from monitoring what is being discussed or planned in the private communications room.

4. Encouragement is offered via pro-terror group action. The private communication affords groups like ISIS to coordinate the specific action the individual was selected for whether it be for a specialized task like being an online facilitator or executing a terror attack.[31]

Within this process, intelligence and law enforcement agencies can monitor and track the communications between terror groups and individuals. "Private" conversations do not stop the ability to monitor the communications, but it does add additional work for agencies that already have limited resources to follow the massive amounts of data being shared each day by groups like ISIS.[32] Use of applications such as FireChat make monitoring communications more difficult because the messages sent are immediately deleted.[33]

Social media is one of the mechanisms that gives ISIS power. The power of connection with people all over the world who want to read, watch, or listen to what ISIS thinks and does on an almost hourly basis is what keeps the "idea" of ISIS alive. ISIS is not going door to door to recruit; rather they are going smartphone to smartphone and by computer to computer. The Internet and social media are what allows ISIS to find what they most need – support, whether it be recruiting actual fighters or to find those who can facilitate the financing and movement of fighters to and from the battlefield. Social media also assists in spreading their global terror campaign by inspiring and directing lone wolf

attacks throughout the world, raising the ISIS brand and getting more attention and interest in their cause.

THE PROVIDERS

A significant problem when determining the best strategy to counter terrorist use of social media is that fact that among all of the social media providers there is not a standard agreement on what constitutes extremism and/or terrorism, and there is not a formalized system to which the United States government coordinates and works with each provider.[34] Also, each provider is different in its views of what is or is not terrorist activity and have differing rules and regulations for when they will suspend or shut down a particular account. The issue the providers find themselves in is how they can continue to provide worldwide platforms that allow for global forums for free speech, discussion, and connection while stopping extremist groups from utilizing these services to further their terror aspirations and goals.[35]

Each provider has its own reputation for how much or how little it does to counter extremist use of their service; each have updated their regulations based upon organizations like ISIS and how they have used specific platforms to post horrific execution videos.[36] For example, after the videos were posted of the execution of journalists James Foley, Steven Sotloff, Peter Kassig, David Haines, and Alan Henning on various social media platforms, Facebook put into affect a process by which all of its users could report content suspected of being terrorist activity which it investigated and in turn closed accounts based upon its terms of service.[37] The differences between various social media outlets and their stance on controlling content is best viewed from the visit of the French Interior Minister Bernard Cazeneuve who met with Google, Facebook, and

Twitter executives after the Charlie Hebdo attack. The purpose of his visit was to allay France's concerns about how extremists were using social media and to work with each company to assist in blocking extreme content. Google and Facebook both re-enforced their policy of shutting down accounts and removing content that was terrorist related. The meeting with Twitter ended with no real agreement to continue to coordinate potential terror related activities and focused on the company's posted guidelines for legal information requests.[38]

The intent of the meetings was to come to a workable solution for procedures on how France and social media outlets can more rapidly close down sites and accounts once it is determined they are being used by extremists. The United States also has received push back in the past from social media companies on increased coordination with the government to counter use of social media by extremist groups. Social media companies monitor accounts for violent and extreme materials, but these companies can find themselves crossing freedom of speech lines quickly, as defining what constitutes extreme or terrorist content is difficult to do.[39] During a private meeting with Senate leaders, Twitter, Facebook, and Google executives all disagreed with legislation that would force them to inform authorities when they flagged terrorist activity on their sites. All argue that this increased coordination will put the companies in a negative legal position if they miss a terror related posting and also lower the public's trust in these companies respecting freedom of speech.[40]

Not only are the social media outlets torn on how best to work with governments to monitor, track, and shut down terrorist operations on social media, but so is the intelligence community (IC). There is conflicting thought on whether shutting down

accounts and sites is the best approach to counter the use by groups such as ISIS. The IC, being focused on analyzing data, argues that not shutting down sites and continued monitoring is the best approach in order to gain additional insight into the groups' intent and operations. J.M. Berger argues in his article, "#Unfollow," that within intelligence circles the thought of closing accounts is not a viable solution as the extremists will just open another account under a different name, and that various government and private security companies depend on continued monitoring of active accounts in order to advance intelligence collection.[41]

In his article, "Countering Islamic State Exploitation of the Internet," David Fidler, an Adjunct Senior Fellow for Cyber Security at the Council on Foreign Relations, discusses the issue of how the US government, working with social media providers raises concerns by certain groups about the infringement of free speech and privacy, but that both government and private parties "can counter the Islamic State's online onslaught through policies anchored in important liberal principles, namely protection of free speech, transparency, and accountability."[42] This is a noble concept and something that the government and private companies can debate and negotiate. In the meantime, terror groups continue their online activities to advance their operations. As this debate lingers into the unforeseen future, the delta created should be covered by a US strategy to counter groups like ISIS on social media.

AN INEFFECTIVE STRATEGY

In mid-February 2015, the Obama administration hosted a three-day summit called Countering Violent Extremism. The summit hosted numerous US based law enforcement (at both the local and federal levels) as well as foreign leaders who have a

stake in fighting groups such as ISIS. One of the topics during the event focused on solutions for countering extremists' use of social media, namely their ability to spread their message and ideology in the vast space of the Internet.[43] President Obama gave closing remarks at the summit. Here, he identified that a main objective of extremist groups is to target younger individuals: "The high-quality videos, the online magazines, the use of social media, terrorist Twitter accounts -- it's all designed to target today's young people online, in cyberspace."[44] The president's comments go on to say that the United States, with its partners, will dedicate additional resources to curb the ability of extremists to continue to recruit and radicalize people to join their ranks and carry out terror acts.

After the summit was over, there were numerous criticisms on the actual benefits of hosting such an event and what end would come of it. As reported by the Congressional blog, "The Hill," the summit fell short of its original intent because the focus was too broad to cover in one event. Specifically, the portion of the summit that was neglected was countering extremist ability to recruit, radicalize, and inspire.[45] Social media is just one aspect of ISIS's lines of operation. The United States does not have a comprehensive strategy that addresses how to destroy the organization, let alone disrupt ISIS's ability to operate through the Internet. During a January 2015 hearing before a Congressional subcommittee on terrorism, it was identified by Massachusetts 9th District Representative Bill Keating that in 2011 the White House identified that terrorist organizations were utilizing social media to "spread hate and violence" and determined that there was a national need for a strategy to combat it.[46]

To date there has not been any formal publication of such a strategy. As Peter Feaver states in one publication, the Unites States' ISIS strategy is "leading from behind."[47] The United States has piecemeal initiatives that focus on countering extremist use of social media, but it is not nested in an overarching strategy on how to combat it. The State Department (Center for Strategic Counterterrorism Communications) has a program called "Think Again Turn Away" which is focused on those individuals who are reaching out to extremist groups and are on the fence in regard to their participation or further radicalization.[48] This campaign is a State Department Twitter account that attempts to counter extremists' views and comments on specific accounts. The program has been viewed overall as ineffective and allows extremists the opportunity to share their views and opinions on US owned platforms which can be counter productive to what the original intent was for the program. Due to the sensitive nature of collection efforts and methods, most of the operations conducted by federal law enforcement agencies such as the FBI and military organizations are classified. The FBI has a more robust program mostly focused on threats within the United States and for those individuals who have been charged with a crime, but those programs are not manned enough to keep up with the extremely large amount of cases that are being followed. Namely, the FBI's Joint Terrorism Task Force (JTTF) focuses on tracking and monitoring terrorist activities both domestically and internationally while sharing the information collected with various intelligence and military units.[49] Other intelligence agencies also have the ability to monitor and track social media usage such as the Central Intelligence Agency (CIA) and National Security Agency (NSA) under different titled

authorities that are generally not open to all domestic agencies and are heavily compartmentalized.

There are also companies contracted by the United States government to follow extremist use of social media to identify trends in terrorist activity, analyze what specific terror groups are doing, and to penetrate groups to get a better sense of who they really are.[50] The incorporation of private industries to support the government's efforts in security efforts is not a new concept. These contracted companies have the manning, technical abilities, and computer systems that can handle the massive amounts of data that other governmental departments might not be able to. The amount of data is a significant problem for the various government organizations that are monitoring accounts. The amount of data is so large that the US government has contracted support from the private technology sector in order to manage and process all of the information. There are also not-for-profit organizations that are active in the fight to counter extremists online. Groups like the Counter Extremism Project have an active online campaign to counter radical use of the Internet to assist in stopping global extremism.[51]

It would appear that there are plenty of organizations ranging from law enforcement, intelligence, military, the State Department, and non-profit organizations that are actively countering terror groups on the Internet. There is clearly no lack of effort, rather a lack of executive leadership to organize these efforts for a common goal or strategy. Executive order 13584 section 2, dictates that State Department's Center for Strategic Counterterrorism Communications (CSCC) "shall coordinate, orient, and inform Government-wide public communications activities directed at audiences abroad and targeted against violent extremists and terrorist organizations, especially al-Qa'ida

and its affiliates and adherents, with the goal of using communication tools to reduce radicalization by terrorists and extremist violence and terrorism that threaten the interests and national security of the United States."[52] If the CSCC is the lead on countering terror groups online, why is there not a whole of government strategy leveraging all of the above organizations that contribute to countering extremism online? The current framework is ineffective and is lacking in a united execution plan led by a US whole of government approach.

It is not lost on the US government that there is a security dilemma in regards to extremist use of social media. Numerous House and Senate Committees receive reports on extremist use of social media, but largely the information provided does not equate to more action by the United States to limit the usage. For example, the House passed an Intelligence Authorization Act for fiscal year 2016, which mandates reporting by the Director of National Intelligence (DNI) specifically on terrorist use of social media. The report provided to the House must cover the following:

- Role to which social media assists in radicalization in the U.S and abroad
- How extremist groups utilize social media
- What if any intelligence value is gained from social media
- How national security is affected by social media[53]

The Senate also has interest regarding social media and terrorism. The Intelligence Authorization Bill does not require the DNI to provide reporting but "does require social media companies to report terrorist activity to the federal government."[54] Other than sound bites airing on the evening news and occasional interest from the House and Senate, none of these efforts indicates that the United States has a policy on how to

counter the use of social media. It is great that policy makers want updates on how the intelligence community views what is being posted on social media, and that the differing agencies analyze actions on the web, but what are we doing with this information? Is the CSCC the right organization to leverage all of the organizations that have capabilities to counter terror groups online, or should that fall to a high-ranking intelligence officer like the Director of National Intelligence (DNI)? There is no formal structure or leadership that supports a comprehensive US strategy, rather piecemeal operations being conducted by the Department of Defense, Law Enforcement Agencies, the IC, and private contracted industry.

AN EFFECTIVE STRATEGY

> "The budget over a three-year period of the Center for Strategic Counterterrorism Communications (CSCC), for example, which I headed for three years, equaled cumulatively the cost of just one Reaper drone. It accomplished some good things with small amounts of money but was always outnumbered and outgunned in the very specific space we are talking about. We need to fund a media counteroffensive appropriately. We don't need to break the bank to fight this adversary in social media but we do need to spend somewhat more than we have and spend more wisely."[55] Alberto M. Fernandez

Legitimacy

In order for the US to have significant effects against terror groups online, it first needs to unite its departments to a common goal and plan to meet that goal. This "whole of government" approach needs to be established within the United States government. A single government agency or department cannot do it alone. In order to do this, Executive Order 13584 (Executive order for CSSC) needs to be expanded to outline the roles and responsibilities of each organization across the government and what the overall strategy is. The president also needs to re-evaluate who leads the US effort against online terror groups and elevate the status of that position to highlight how important this mission set

is to the United States. The administration also has to be clear that the US strategy encompasses diplomatic, military, economic, and cyber components that, coupled together, will achieve success in the defeat of terror groups like ISIS and curb global terrorism. Each component needs its own independent legitimacy as a portion of the over-arching strategy in order for it to have the support needed to execute its mission. The US government cannot build an international coalition to counter terror groups operating online until it gets itself together first.[56]

Expand role of the US Military

The US military has a tremendous cyber capability within US Cyber Command and in various special mission units in the US military.[57] While the US government adjusts to the renewed focus and emphasis on combating terror groups online, the US military can fill the gaps and start to have effects. In order to do this, the US military needs to prioritize social media efforts higher than it historically has done in the past. US Cyber Command can re-structure itself to focus more on social media collection while still maintaining its ability to protect the United States from state and non-state hackers. Additionally, military units that currently have a cyber mission can also prioritize social media targeting at every level. The US has numerous DoD Regional Task Forces (RTF's) that are deployed worldwide.[58] Each has its own unique mission and the vast majority has a cyber component. All RTFs work with US law enforcement, intelligence agencies, and US Embassies and share intelligence collection efforts. By expanding the mission to cover social media, each RTF will have the ability to monitor and track extremist use of social media in their Area of Operation (AO). For example, an RTF stationed in Germany, working with its intelligence partners, will have the ability to identify

individuals in the area that are being radicalized or have intent to conduct an attack in the area. The various RTFs will start to build a global picture of where radicalized individuals are and whom they are getting guidance from. This global network will give the US military the ability to Find and Fix (locate) individuals in their AO and characterize the threat they pose based upon the command structure of the assumed terror organization of which they are a part.[59] Analysts would be able to map the network and identify the central leadership compared to an "online" solider or sympathizer.[60]

At each location, the RTFs will have at some level a relationship with a foreign military unit. This partnership can be expanded to develop a host nation counter cyber program that would allow for not only monitoring terrorist use of social media but counter messaging from the perspective culture and language used in that country. Also, the partner units could have the ability to arrest individuals who are determined to join groups like ISIS or who are planning terror attacks. By regional partnership with foreign countries and expanded cyber capabilities, the US military utilizing the system currently in place could have greater effects in countering terrorist groups online and be incorporated into a broader US coalition. This is currently taking place in a variety of countries, but the US military has limited authorities to target online terrorist personalities rather than solely using their Internet activity to monitor and track them.

Expanded Authorities

The US military in recent years has been heavily involved in global counterterrorism operations. The military nominates targets based upon gathered intelligence to gain authorities to target specific individuals who pose a threat to the United States or US persons or property aboard. In order to gain authorities to target an

individual, the military has to submit a target package that outlines in detail why that individual should be targeted. The process to nominate an individual is lengthy and gets scrutiny from both senior military leaders and senior civilians in the administration. The president has several supporting documents that authorize nominating targets, namely the 2001 Authorization for the Use of Military Force (AUMF), Article 51 of the UN Charter, and Article II of the US Constitution.[61] In recent years, the administration has utilized the 2001 AUMF, which authorizes the President "to use all necessary and appropriate force in pursuit of those responsible for the terrorist attacks."[62] After approval is gained for the nominated individual, the military has authorization to conduct operations against the individual in order to capture or kill them.

The AUMF process has application in combating extremist use of social media. If government agencies and military units are monitoring and tracking extremists online, the military should seek to gain AUMF on key online facilitators, recruiters, and those who radicalize would be terrorists. The military for years has targeted facilitators and recruiters in both Iraq and Afghanistan in an attempt at dismantling a terror network from top to bottom.[63] In order to have an effect on the top of a terror group, action must be conducted at the lower and middle levels. The AUMF nomination is mostly comprised of intelligence on why the targeted individual presents a threat to the United States and its citizens abroad. Do online recruiters and facilitators pose a direct threat to the United States? The answer is it depends. If the extremist has the ability to coordinate and facilitate an attack targeting the United States, then, yes, the ability to gain AUMF approvals is probable. However, if there is no certain connection that the extremist is engaged in attack planning or coordination, then the process is more complicated.

Very few people would argue that detaining extremists that are involved in online recruiting, facilitating, and radicalizing individuals to participate in terror activities is not a sound concept. There is great debate about the AUMF process and whether or not it has been managed properly since 9/11. The reason why is there are several loopholes that the military and other agencies can use to gain authorities, one of which would be helpful in getting AUMF for online extremist members. Continuous Combat Function (CCF) refers to individuals who provide essential duties (functions) to groups identified as hostile.[64] Individuals who are determined to be CCF are targetable by use of military force due to their activities with a group determined to be hostile. Another avenue to achieve authorities against online priority targets is to classify that the extremists are "functional members" of a terror group.[65] The main issue currently is that there is no standing AUMF for ISIS, making gaining authorities on specific ISIS members, like the senior media members, difficult.

President Obama is currently working with the House to develop an AUMF proposal strictly targeting ISIS. This new AUMF is long overdue and should address and classify online facilitators, recruiters, and those extremists who radicalize individuals online.[66] Until a comprehensive AUMF is approved for ISIS, the military should pursue authorities using the CCF and functional membership avenues in order to have the ability to do something to take online extremists off the net. In the ISIS command structure, leadership and ISIS members of the ISIS digital army would fall within the CCF and membership avenues, which would make them eligible for AUMF. The intelligence communities in conjunction with the various RTFs have the needed data and analytical

capabilities to determine which online terror personality is eligible for CCF or membership.

Find, Fix, Finish, Exploit, Analyze

The legal framework to counter ISIS is a work in progress and should cover recruitment and facilitation in support of ISIS as illegal.[67] The US military would not seek to gain AUMF authorities on all online extremists, rather it would seek those who meet specific criteria. During the monitoring and collection of online and social media activities, analysts in the military and intelligence agencies will have the ability to piece together who the most significant online members are. Based upon that, AUMF packages would be developed and submitted for approval. Just because the US military has AUMF authorities does not mean that US service members will conduct an operation to capture the individual. Working by, with, and through foreign counterparts' counterterrorism (CT) units and law enforcement agencies (LEAs), the US can influence a foreign nation to act to arrest the extremists in their own country. This was recently demonstrated across Europe when 15 members of ISIS were detained in several raids after law agencies monitored them online and identified them as planning multiple attacks.[68] As mentioned earlier, the US military already has RTFs and close relationships with CT and LEAs all over the world. More than likely, if an individual is on the US's radar, a foreign nation is probably aware of them. AUMF is a leverage tool and a mechanism to get the foreign nation to conduct an operation against the individual. AUMF is an indicator of how important the suspected extremist is to the US. AUMF is somewhat comparable to LEA's obtaining warrants for a suspect's arrest. Policing agencies do not gain warrants for random people, rather they gain warrants for suspects who are deemed to be connected to

crime or have committed a crime. Once AUMF is authorized, it sends a clear message to the foreign nation and illustrates that the US is willing to conduct unilateral action if needed to capture the individual. By working with foreign partners and letting them conduct operations resulting in the capture of extremists or extremist facilitators sends a message to ISIS (or affiliated groups) and the world that conducting terror behind a computer screen is just as dangerous as fighting in the ranks in Syria and Iraq in regard to the potential for being detained or killed by international coalition forces.[69]

Capturing a terrorist or key facilitator is critically important in the targeting cycle. The ability to interview the individual and to obtain his/her electronic devices, documents, and materials, not only gives the IC a better understanding of how the terrorist group operates, but it also spreads fear within the terrorist organization. The material gathered during Sensitive Site Exploitation (SSE) is very valuable, but the ability to interview the individual, if they do in fact want to talk, is even more valuable. The information and understanding of how groups like ISIS organize, direct, and execute its social media and online campaign will lead to greater ability to counter it and destroy its ability to continue to operate in the cyber realm. The US military has the capabilities needed to fill the current gap in activities to counter terror groups online while the US government re-focuses its efforts into a more effective strategy.

International Whole of Government Approach – Coalition

The US cannot tackle this alone and must work with its Muslim nation partners to defeat ISIS online.[70] Muslim country participation is essential in the fight against terror groups on the web. Muslim leaders and clerics must be part of the effort in order for it to succeed.[71] Efforts to counter extremists must have a Muslim voice; the US cannot

adequately represent this population alone. Partnership with the international Islamic community will increase the legitimacy of the effort and provide a better understanding of the Islamic world, which is needed to effectively counter ISIS's ideology.[72] The coalition must also harness governmental and non-governmental organizations to understand best practices, implement technological expertise, and offer varying perspectives to the problem. The goal of the coalition should be balanced in the sense of not being too heavy on "US" voice and "government," rather it has to have a Muslim perspective and a non-government approach in order to gain credibility with potential followers. Participation by non-government organizations will also cultivate fresh ideas and approaches that would not be developed within a coalition of solely government departments. The US needs to be the leader to develop a coalition that is focused and effective in countering groups like ISIS online. The coalition has to be sensitive to religion and have a voice that is balanced in order to draw the attention of those who are being radicalized. If the message is too heavily pushed by government organizations like the Department of State or a partner country's foreign minister's office, then it will not be as powerful as an organization that is free of government clout. It also has to span and leverage political leaders, religious figures, militaries, tech companies, public relations experts, survey firms, and global LEAs. Together these organizations can form an international whole of government approach, a coalition that can truly counter terror groups online that is balanced and has the right voice to gain credibility.

These efforts have to not only focus on the global fight but also at the community level. Individual communities must have the ability to counter radicalization and counter message at the lowest level. More than likely local LEAs will miss signals that

individuals in communities are self-radicalizing or are being radicalized online, but members of the community will notice.[73] According to Professor Anders Strinberg of the the Naval Postgraduate School's Center for Homeland Defense and Security, in order for the local community to help LEA's counter radicalization there needs to be a level of "trust and integration" between law enforcement and the Muslim community.[74] The coalition has to have a mechanism to assist community and religious leaders at the community level, but cannot do so if there is not trust between the two groups. The coalition can identify areas or communities that are more susceptible to radicalization and utilize community outreach programs to first build trust and then mutually counter the radicalization.

Another important aspect of combating terror groups is a rehabilitation program for former members of terror organizations. Historically these programs have had limited success, but if former members could voice their opposition to groups like ISIS online, it could assist in getting the true reality of what it is like to be a member of the organization in order to counter the romantic idea.[75] Firsthand reporting from former terror groups' members must be a part of the counter-messaging campaign in order to refute claims by the group and expose the true realities of being a member of a terror organization.[76] Mubin Shaikh is an example of how this concept can work and assist in the counter-narrative online. Mr. Shaikh was born in Canada, to devout Muslim Indian immigrants and turned toward radical Islam through his high school years. He eventually was radicalized, moved to Quetta, Pakistan, quickly adopted a pro-AQ ideology, and assisted in online recruitment of young Muslims. In 2004, Mr. Shaikh became disillusioned with the mindset of AQ and began working with Canadian Intelligence Services to counter

online recruitment to include both undercover and online infiltration operations into forums and websites organized by terror groups. His efforts led to 11 radicalized Canadians being convicted of terrorism charges in 2005.[77]

Developing such a coalition is extremely challenging but offers the most chance of success. The United States and partner countries should do whatever they can to support non-government and not-for-profit organizations to support their efforts to combat terror groups online.[78] Assistance, such as developing funding lines or grants to assist non-profit/non-government organizations in the fight against radicalization online, will help in building a team that has the needed expertise in technology, culture, and religion that will make the coalition creditable, an attractive alternative to terror groups, and a threat to the groups that seek recruits. The US must do everything in its power to empower and lead the coalition within its borders and in the international community.[79] ISIS will continue to expand its cyber operations and intensify its "cyber-jihad" to recruit, plan attacks, and inspire lone wolf attacks worldwide. The problem will only get worse, and the time it takes for an effective coalition to organize itself will only benefit terror groups to further advance their abilities online.

OPPOSITION

There are very few people who disagree with fighting ISIS on land with sustained airstrikes and limited ground forces; however, there is debate on whether the US should spend effort combating extremist groups online, to what end and at what cost to our civil liberties and privacy.[80] There are members of the intelligence community who advocate continued monitoring of extremist accounts vice shutting them down to gain a better

understanding of the network and future operations.[81] Websites and social media serve as a means to monitor, track, and analyze extremist groups and their followers.[82] Certain members of the intelligence community believe that the understanding and increased knowledge allowed by continuous monitoring outweighs shutting down accounts and websites. Also, others claim that shutting down accounts is extremely difficult to manage, due to the large number of accounts created and the rapid ability for group members to re-open accounts after they were shut down by social media outlets.[83] The ability of extremists to quickly get back online has created an environment for intelligence and counterterrorism analysts that is referred to as "whack-a-mole" and is an ineffective strategy to counter groups like ISIS on the Internet.[84]

Others believe that ISIS will eventually lose following due to its increasing violent nature and horrific acts. Scholars like Dr. Max Abrahms believe that the social media campaign by ISIS has been blown out of proportion by so called "social media alarmists."[85] Dr. Abrahms argues that social media has not been proven to assist the group and that continued use of violent media content will only strengthen the growing coalition who is conducting military operations against it resulting in tremendous losses for ISIS in Iraq and Syria. He also argues that the anti-ISIS coalition should step back from stopping the group online because their media campaign is counter-productive to its original intent to gain worldwide support.[86] Clint Watts, a Fox Fellow at the Foreign Policy Research Institute's Program on the Middle East, also agrees that terror groups like ISIS will eventually lose support due to its brutal tactics and ideology. Mr. Watts believes that the US and international coalitions should "contain" ISIS instead of countering the group.[87] Containing ISIS, Watts argues, would lead to the alienation of the

local community resulting in local militias combating ISIS rather than coalition forces.[88] This strategy aligns with Dr. Abrahms' in the sense that ISIS will eventually defeat itself if properly contained on land or on the Internet.

Clint Watts also believes that the current US strategy to counter terror groups online is ineffective and is plagued by a "whole of government trap."[89] Watts believes that the "whole of government" approach has too many challenges that impede any sort of advancement in the fight to counter terror groups. Watts also argues that DoD units are not the optimal organization to take the lead on countering social media due to a lack of expertise in the field and the Department of State, who has the proper authorities, will never get the needed resources to properly execute an effective counter-narrative.[90] Watts also believes that US LEA's lack needed authorities, and the intelligence community is hampered by growing privacy concerns. The "whole of government" approach also generates an environment that is slow, inflexible, and lacks credibility due to the large nature of US government bureaucracy.[91] Watts believes that an effective counter-narrative has to focus primarily on defectors from the terror group and lead from DoS's CSSC program.[92]

After the Edward Snowden leaks in June 2013, there has been increasing concern and debate about the balance between national security and privacy.[93] The leaking of sensitive information about how the US conducts intelligence collection, specifically cyber collections, has escalated a debate about whom the US should and should not spy on in regard to personal communications between US citizens and foreigners.[94] Opponents to mass data collection believe that it is a violation of personal rights to have their data collected while proponents believe that mass collection will assist in stopping

the next spectacular terror attack and increasing national security.[95] Regardless, in order to move forward there has to be a balance between individual privacy online and the US government's ability to monitor suspected terrorist activities in the cyber realm. The IC, specifically the National Security Agency (NSA), remains the most equipped and capable force to combat terror groups online, but has been hampered in recent years after leaks about specific collection programs.[96] These leaks have increased scrutiny on the IC and have hampered efforts to counter groups like ISIS, not only over privacy concerns, but also due to the fact that terrorist organizations changed their communications procedures after the Snowden leaks, making it harder for the IC's collection efforts to monitor their traffic.[97]

Global security today is largely dominated by technology, which provides terrorist groups opportunities on how to utilize said technology to radicalize, recruit, and inspire attacks, but it also affords intelligence agencies opportunities to exploit that usage.[98] The tempo of evolving technology and use of social media has outpaced the US government's ability to effectively provide security while ensuring individual privacy. The scope of this conversation is beyond this paper, but it is critically important that this debate be resolved in order to meet a much-needed balance between online surveillance collection and individual privacy rights. The US must reach a compromise in dealing with social media companies to ensure that the proper amount of data is being shared in a method that protects US citizens, remains transparent, has the proper amount of Congressional oversight, and avoids abuse by the intelligence community.[99]

The US military is not the final recourse for this problem set. An effective international whole of government approach is the solution. As noted in this paper,

building such a coalition is an extremely difficult task and requires a clear end state, legitimacy, and Muslim partner country participation. Using the US military is an interim strategy that will leverage existing capabilities to disrupt the ability of terror groups to exploit social media to benefit its operations. The expanded use of the US military allows the coalition the ability to apply pressure in a timely fashion. Military operations will provide much needed time for the international coalition to organize itself with a shared vision and organization needed to carry the mission forward. US military involvement will provide the opportunity to build coalition partner capability to disrupt terrorist operations online furthering developing a true international ability. The US military's role will eventually transition to a supporting, advisory function as the international coalition matures and other governmental departments take primacy on the overall mission.

Another key aspect of US military involvement in countering extremism online is a transition from "contesting the space" to a more disruptive strategy. The international coalition is not yet prepared to disrupt terror groups online, but the US military is ready to take this step. Just as increased kinetic strikes targeting key ISIS command and control locations and infrastructure, so too will a disruptive online offensive targeting key online terrorist facilitators resulting in diminished operational capability. Expanding pressure on ground, air, and cyber space will have a more cumulative effect on terror groups like ISIS. The cyber realm must become just as dangerous for terror groups members, radicalizers, facilitators, and recruiters as the battlegrounds of Syria and Iraq. The only way to do this is to transition to a disruptive strategy on the World Wide Web.

This topic must continue to be analyzed in order to find a sustainable solution. More study needs to be conducted in the academic, military, and governmental realms in order to fully understand the problem and what the best approach is to effectively combating it. The rapid development of technology will make this a difficult task, but it must be addressed properly as the fight against terrorism continues.

Notes

[1]CBS News, "Why it's so difficult to counter ISIS on social Media," *CBSnews.com*, June 23, 2015, http://www.cbsnews.com/news/why-so-difficult-counter-isis-social-media/.

[2]Holly Yan, "Texas attack: What we know about Elton Simpson and Nadir Soofi," *CNN.com*, May 5, 2015, http://www.cnn.com/2015/05/05/us/texas-shooting-gunmen/.

[3]The New York Times, "Joining the Fight in Somalia," *nytimes.com*, October 30, 2011, http://www.nytimes.com/interactive/2009/07/12/us/20090712-somalia-timeline.html?_r=1&.

[4]Ritz Katz, "Texas attack: The chain of terror tweets that led to Elton Simpson rampage at Draw Mohammed contest," May 6, 2015, *ibtimes.co.uk*, http://www.ibtimes.co.uk/texas-attack-chain-terror-tweets-that-led-elton-simpson-rampage-draw-mohammed-contest-1499922.

[5]Cathy Burke, "American ISIS Recruiter Linked to Texas Terror Shootings," *newsmax.com*, May 6, 2015, http://www.newsmax.com/Newsfront/Elton-Simpson-fugitive-recruiter-Miski/2015/05/06/id/643089/.

[6]Editorial Board, "Social Media Sites Don't Need government to Shut Down Terrorists," *The Washington Post*, December 13, 2015, https://www.washingtonpost.com/opinions/social-media-sites-dont-need-government-to-shut-down-terrorists/2015/12/11/90c5fe86-a029-11e5-8728-1af6af208198_story.html.

[7]Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges*. (Washington, DC: United States Institute of Peace Press, 2006), 4.

[8]Thomas Rodebaugh, US State Department, Director for Digital Outreach, Center for Strategic Counterterrorism Communications, interview by LCDR W. A. Shafer, January 6, 2016.

[9]Rodebaugh, interview by LCDR W. A. Shafer, January 6, 2016.

[10]J.M. Berger, Nonresident Fellow at the Brookings Institute and author, interview by LCDR W.A. Shafer, December 28, 2015.

[11]P.W. Singer and Emerson Brooking, "Terror on Twitter: How ISIS is taking war to social media – and social media is fighting back," *Popular Science, http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media.*

[12]Reprentative John Ratcliffee, U.S. Congress. House. *Hearing on Homeland Security*. 114th Cong., 2015.

[13]James Van de Velde, "Crash Their Comms," *The American Interest,* Vol. X, No. 6, July/August 2015, 35-36.

[14] Senator Carper, Thomas R, U.S. Congress. Senate. *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment, Hearing before the Senate Committee on Homeland Security & Governmental Affairs*. 114th Cong., 2015.

[15]Peter Bergen, "Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment, Hearing before the Senate Committee on Homeland Security & Governmental Affairs," May 7, 2015. http://www.hsgac.senate.gov/hearings/jihad-20-social-media-in-the-next-evolution-of-terrorist-recruitment.

[16]"Al-Shabaab," National Counter Terrorism Center, *Terrorist Groups*, September 23, 2015, http://www.nctc.gov/site/groups/al_shabaab.html.

[17]"Al-Qa'ida In the Arabian Peninsula (AQAP)," National Counter Terrorism Center, *Terrorist Groups*, September 23, 2015, http://www.nctc.gov/site/groups/aqap.html.

[18]Richard Adams, "Anwar al-Awlaki killed in Yemen – as it happened," *theguardian.com*, September 30, 2011, http://www.theguardian.com/world/blog/2011/sep/30/anwar-al-awlaki-yemen-live.

[19]Shane, Scott, "The Lessons of Anwar al-Awlaki." *The New York Times Magazine*, August 27, 2015. http://www.nytimes.com/2015/08/30/magazine/the-lessons-of-anwar-al-awlaki.html.

[20]David Johnson and Scott Shane, "U.S. Knew of Suspect's Tie to Radical Cleric," *NYtimes.com*, November 9, 2009, http://www.nytimes.com/2009/11/10/us/10inquire.html.

[21]Ambinder, Marc, "Al Qaeda's First English Language Magazine Is Here," *The Atlantic*, June 30, 2010, http://www.theatlantic.com/international/archive/2010/06/al-qaedas-first-english-language-magazine-is-here/59006/.

[22]"Issues of Inspire Magazine," *Anti-Defamation League*, September 23, 2015, http://www.adl.org/combating-hate/m/inspire-magazine/c/issues-of-inspire-magazine.html?referrer=https://www.google.com/.

[23]U.S. Congress. House, *The Evolution of Terrorist Propaganda: The Paris Attack and Social Media*: *Hearing before the Subcommittee on Terrorism, Nonproliferation, and Trade on the Committee on Foreign Affairs.* 114th Cong., 2015.

[24]"Al-Qa'ida in Iraq (AQI)," The National Counterterrorism Center, *Terrorist Groups*, September 23, 2015, http://www.nctc.gov/site/groups/aqi.html.

[25]Weaver Ann, Mary, "The Short, Violent Life of Abu Musab al-Zarqawi," *The Atlantic*, June 8, 2006, http://www.theatlantic.com/magazine/archive/2006/07/the-short-violent-life-of-abu-musab-al-zarqawi/304983/.

[26]Max Abrahms, "Why the Islamic State actually stinks at social media," *Opencanada.org*, April 20, 2015, https://www.youtube.com/watch?v=nzL9tdUjcS8.

[27] Anna Brugulis, "Stanley McChrystal: ISIS reaches 100 million people a day through social media campaign,"*Punditfact.* Accessed November 4, 2015, http://www.politifact.com/punditfact/statements/2015/jun/25/stanley-mcchrystal/stanley-mcchrystal-isis-reaches-100-million-people/.

[28]J.M. Berger and Jonathon Morgan, *The ISIS Twitter Census.* The Brookings Project on U.S. Relations with the Islamic World, No. 20. March 2015.

[29]Karen Yourish, Derek Watkins, and Tom Giratikanon, "Where ISIS Has Directed and Inspired Attacks Around the World,". *The New York Times*, updated August 20, 2015, http://www.nytimes.com/interactive/2015/06/17/world/middleeast/map-isis-attacks-around-the-world.html?_r=0.

[30]Erick Stakelbeck, *ISIS Exposed*. (Washington, DC: Regnery, 2015), 200-201.

[31]J.M. Berger, "Tailored Online Interventions: The Islamic State's Recruitment Strategy," *CTC Sentinel*, October 2015, Vol. 8, Iss. 10, 21-25.

[32]Timothy Stenovec, "Messaging Apps Like Tango, Whatsapp and Skype Not Immune to Government Reach," Huffington Post. Updated June 7, 2013. http://www.huffingtonpost.com/2013/06/07/messaging-apps-government-reach_n_3399316.html.

[33]James Van de Velde, "Crash Their Comms," *The American Interest*, Vol. X, No. 6, July/August 2015, 35.

[34]Jessica Stern and J.M. Berger, *ISIS: The State of Terror* (New York: HarperCollins, 2015), 134-135.

[35]Scott Higham and Ellen Nakashima, "Why the Islamic State leaves tech companies torn between free speech and security," *Washingtonpost.com*, July 16, 2015, https://www.washingtonpost.com/world/national-security/islamic-states-embrace-of-social-media-puts-tech-companies-in-a-bind/2015/07/15/0e5624c4-169c-11e5-89f3-61410da94eb1_story.html?kmap=1.

[36]Julia Greenberg, "Why Facebook and Twitter Can't Just Wipe Out ISIS Online," *Wired*, November 21, 2015, http://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/.

[37]"Scott Higham and Ellen Nakashima, "Why the Islamic State leaves tech companies torn between free speech and security," *Washingtonpost.com*, July 16, 2015, https://www.washingtonpost.com/world/national-security/islamic-states-embrace-of-social-media-puts-tech-companies-in-a-bind/2015/07/15/0e5624c4-169c-11e5-89f3-61410da94eb1_story.html?kmap=1.

[38]Associated Press, "French minister meets with Google, Facebook, Twitter," *The Indian Express*, June 21, 2015, http://indianexpress.com/article/world/europe/french-minister-meets-with-google-facebook-twitter/.

[39]Brain Naylor, "What Can-Or Should-Internet Companies Do To Fight Terrorism?" *NPR*, December, 15, 2015, http://www.capradio.org/news/npr/story?storyid=459370449.

[40]"Could Twitter stop the next terrorist attack?" Anne Flaherty, *Associated Press*, last modified July 24, 2015, https://www.yahoo.com/tech/s/could-twitter-stop-next-terrorist-attack-072946810--finance.html?nf=1.

[41]J.M. Berger, "#Unfollow," *Foreign Policy*, February 20, 2013, http://foreignpolicy.com/2013/02/20/unfollow/.

[42]"The War On Terrorists' Tweets," David Fidler, *Defense One*, last modified July 17, 2015, http://www.defenseone.com/technology/2015/07/war-terrorists-tweets/118087/.

[43]"FACT SHEET: The White House Summit on Countering Violent Extremism," The White House Office of the Press Secretary, accessed September 30, 2015. https://www.whitehouse.gov/the-press-office/2015/02/18/fact-sheet-white-house-summit-countering-violent-extremism.

[44]"Remarks by the President in Closing of the Summit on Countering Violent Extremism," The White House Office of the Press Secretary, February 18, 2015, https://www.whitehouse.gov/the-press-office/2015/02/18/remarks-president-closing-summit-countering-violent-extremism.

[45]Meryl Chertoff, "Notes from the White House Summit on Countering Violent Extremism," *The Hill* (blog), February, 26, 2015, http://thehill.com/blogs/congress-blog/homeland-security/233831-notes-from-the-white-house-summit-on-countering-violent.

[46]U.S. Congress. House. *The Evolution of Terrorist Propaganda: The Paris Attack and Social Media*: *Hearing before the Subcommittee on Terrorism, Nonproliferation, and Trade on the Committee on Foreign Affairs.* 114th Cong., 2015.

[47]Feaver, Peter D, "Obama's Problem with ISIS Isn't an Incomplete Strategy – It's a failing one," *Foreign Policy*, June 9, 2015, http://foreignpolicy.com/2015/06/09/obamas-problem-with-isis-isnt-an-incomplete-strategy-its-a-failing-one/.

[48]Rita Katz, "The State Department's Twitter War With ISIS is Embarrassing," *Time*, September 16, 2014, http://time.com/3387065/isis-twitter-war-state-department/.

[49]"Protecting America From Terrorist Attack," Federal Bureau of Investigation, accessed September 30, 2015, https://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs.

[50]Yasmin Tadjdeh, "Government, Industry Countering Islamic State's Social Media Campaign (UPDATE)," *National Defense Magazine*, December 2014, http://www.nationaldefensemagazine.org/archive/2014/December/Pages/GovernmentIndustryCounteringIslamicStatesSocialMediaCampaign.aspx.

[51]Counter Extremism Project, *Counter Extremism Project*, October 1, 2015, http://www.counterextremism.com/.

[52]White House. https://www.whitehouse.gov/the-press-office/2011/09/09/executive-order-13584-developing-integrated-strategic-counterterrorism-c.

[53]Congress.gov, *Summary: H.R. 2596 Intelligence Authorization Act for Fiscal Year 2016*. 114th Congress, June 17, https://www.congress.gov/bill/114th-congress/house-bill/2596.

[54]U.S. Congress, *Intelligence Authorization Act for Fiscal Year 2016*. 114th Congress, June 17, 2015. Intelligence Authorization Act for fiscal year 2016, https://www.congress.gov/bill/114th-congress/house-bill/2596/text.

[55]Alberto M. Fernandez, *Social Media: An Evolving Front in Radicalization*, Hearing before the House Oversight and Government Reform Committee, Subcommittee on National Security, 114th Cong., 2015.

[56]Barack Obama, "Remarks by the President on the Military Campaign to Destroy ISIL,"(speech, The Pentagon, Washington, DC, December 14, 2015. https://www.whitehouse.gov/the-press-office/2015/12/14/remarks-president-military-campaign-destroy-isil.

[57]Shane Harris. *@War: The Rise of the Military-Internet Complex.* (New York: Houghton Mifflin Harcourt, 2014), 124-125.

[58]Dana Priest and William M. Arkin, "Top Secret America: A look at the military's Joint Special Operations Command," *The Washington Post*, September 2,

2011, https://www.washingtonpost.com/world/national-security/top-secret-america-a-look-at-the-militarys-joint-special-operations-command/2011/08/30/gIQAvYuAxJ_story.html.

[59]Harris, 79.

[60]Jerad Cohen, "Digital Counterinsurgency: How to Marginalize The Islamic State Online," *Foreign Affairs*. November/December 2015. https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency.

[61]Public Law 107-40, 107th Congress. Sec. 2. Authorized Use of Military Force. http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/pdf/PLAW-107publ40.pdf.

[62]Ken Gude. "Understanding Authorizations for the Use of Military Force." *Center for American Progress.* September 24, 2014. https://www.americanprogress.org/issues/security/report/2014/09/24/97748/understanding-authorizations-for-the-use-of-military-force/.

[63]William C. Banks and Peter Raven-Hansen, *667 Targeted Killing and Assassinations: The U.S. Legal. University of Richmond Law Review Association, 2003, http://www.americanbar.org/content/dam/aba/migrated/2011_build/law_national_security/westlaw_document143350.authcheckdam.pdf.

[64]Kenneth Watkin, "Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities," Interpretive Guidance, *New York University of International Law and Politics.* Vol. 42:641. 2010, 655-657.

[65]Jens David Ohlin. *The Assault on International Law*. (New York: Oxford University Press, 2015), 170-171.

[66]Peter Beinart. "Why Won't the GOP Declare War on ISIS?" *The Atlantic.* May 28, 2015.

[67]Fergus Hanson, "Countering ISIS in Southeast Asia: The case for an ICT offensive," *University of Western Australia - Perth USAsia Centre*. February 2015.

[68]Massimiliano Di Giorgio, "European swoop seizes 15 Islamists police say planning attacks," *Reuters*, November 12, 2015, http://uk.reuters.com/article/2015/11/12/uk-italy-arrests-idUKKCN0T10NZ20151112.

[69]Jerad Cohen, "Digital Counterinsurgency: How to Marginalize The Islamic State Online," *Foreign Affairs*. November/December 2015. https://www.foreignaffairs.com/articles/middle-east/digital-counterinsurgency.

[70]Martin Matishak, "Sanders: US shouldn't have to fight ISIS alone," *The Hill* (blog), August 13, 2014,

http://thehill.com/policy/defense/215085-sanders-us-abroad-must-unite-to-drive-back-isis.

[71]Stakelbeck, 206.

[72]Stakelbeck, 189.

[73]Martin Kaste, "2 LA Counterterrorism Cops Build Bridges With Muslin Community," *NPR*, December 21, 2015, http://www.npr.org/2015/12/21/460536774/2-la-counterterrorism-cops-build-bridges-with-muslim-community.

[74]Anders Strinberg, correspondence with LCDR W. A. Shafer, January, 2016.

[75]Marisa L. Porges, "The Saudi Deradicalization Experiment," *Council on Foreign Relations*, January 22, 2010, http://www.cfr.org/radicalization-and-extremism/saudi-deradicalization-experiment/p21292#.

[76]P.W. Singer and Emerson Brooking, "Terror on Twitter: How ISIS is taking war to social media – and social media is fighting back," *Popular Science, http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media.*

[77]Mubin Shaikh, Testimony to the U.S. Congress. Senate. *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment, Hearing before the Senate Committee on Homeland Security & Governmental Affairs*. 114th Cong., 2015.

[78]David P. Fidler, "Countering Islamic State Exploitation of the Internet," *Council on Foreign Relations*, June 2015, http://www.cfr.org/cybersecurity/countering-islamic-state-exploitation-Internet/p36644.

[79]Stakelbeck, 190-191.

[80]U.S. Department of State, Counterterrorism Department. Anonymous interview.

[81]J.M. Berger, Nonresident Fellow at the Brookings Institute and author, interview by LCDR W.A. Shafer, December 28, 2015.

[82]Van de Velde, 39.

[83]Stern and Berger, 161-162.

[84]Aki Peritz, "What Whac-A-Mole Can Teach Us About How to Fight Terrorism," *Foreign Policy*.com, August 12, 2015, http://foreignpolicy.com/2015/08/12/what-whac-a-mole-can-teach-us-about-how-to-fight-terrorism/.

[85]Max Abrahms, "Why the Islamic State actually stinks at social media," OpenCanada.org, April 20, 2015, https://www.opencanada.org/features/why-the-islamic-state-actually-stinks-at-social-media/.

[86]Dr. Max Abrahms, "Understanding ISIS: Myth and Realities," YouTube video, May 26, 2015, https://www.youtube.com/watch?v=nzL9tdUjcS8.

[87]Clint Watt, "Let Them Rot: The Challenges and Opportunities of Containing rather than Countering the Islamic State," *Perspectives on Terrorism*, Vol. 9, Iss. 4. (August 2015): 156.

[88]Watts, 157.

[89]William McCants and Neil Aggarwal, "Experts weigh in (part 6): Can the United States counter ISIS propaganda?" *The Brookings Institute*, July 8, 2015, http://www.brookings.edu/blogs/markaz/posts/2015/07/08-us-counter-isis-propaganda-aggarwal, 3.

[90]McCants and Aggarwal, 3.

[91]McCants and Aggarwal, 4.

[92]Clinton Watts, "Interview with Clinton Watts," interviewed by C-SPAN, *Washington Journal*, August 28, 2014, http://www.c-span.org/video/?321100-3/washington-journal-clinton-watts-us-response-isis.

[93]Jon L. Mills, "The Future of Privacy in the Surveillance Age," in *After Snowden*, ed. Ronald Goldfarb, (New York: St Martin's Press, 2015): 206.

[94]Ronald Goldfarb, introduction to *After Snowden*, edited by Ronald Goldfarb (New York: St Martin's Press:, 2015): 19.

[95]Michael Morell, *The Great War of Our Time: The CIA's Fight Against Terrorism from Al Qa'ida to ISIS,* New York: Twelve, 2015), 287.

[96]Morell, 294.

[97]Jon L. Mills, "The Future of Privacy in the Surveillance Age," in *After Snowden*, ed. Ronald Goldfarb, (New York: St Martin's Press, 2015): 222-227.

[98]Mills, 229.

[99]Mills, 226-229.

Bibliography

Interviews and correspondence

Abrahms, Max. Professor of Political Science at Northeastern University. Personal email to author, November 4, 2015.

Berger, J.M. Nonresident Fellow at the Brookings Institute and author, interview by LCDR W.A. Shafer, December 28, 2015.

Feierstein, Gerald. US State Departments Principle Deputy Assistant Secretary (PDAS) Near East Division, interview by LCDR W.A.Shafer, January 6, 2016.

Rodebaugh, Thomas. US State Department, Director for Digital Outreach, Center for Strategic Counterterrorism Communications, interview by LCDR W. A. Shafer, January 6, 2016.

Bureau of Counterterrorism, Department of State, interviews by LCDR W. A. Shafer, January 6, 2016.

Strindber, Anders. Professor at the Naval Postgraduate School Center for Homeland Defense and Security. Personal email to the author, December 23, 2015.

Media outlets

Associated Press

CBS News

CNN News

International Business Times

National Public Radio

New York Times

Reuters

The Atlantic

The Guardian

The Hill

The Indian Express

The Washington Post

Primary sources

Berger, J.M. *Social Media: An Evolving Front in Radicalization*, Hearing before the House Oversight and Government Reform Committee, Subcommittee on National Security. 114th Cong., 2015.

Carper, Thomas R, Senator, U.S. Congress. Senate. *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment*, Hearing before the Senate Committee on Homeland Security & Governmental Affairs. 114th Cong., 2015.

Ratcliffee, John, Representative, U.S. Congress. House. *Hearing on Homeland Security*. 114th Cong., 2015.

Shaikh, Mubin. Testimony to the U.S. Senate. *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment, Hearing before the Senate Committee on Homeland Security & Governmental Affairs*. 114th Cong., 2015.

U.S. Congress. House. *The Evolution of Terrorist Propaganda: The Paris Attack and Social Media*: *Hearing before the Subcommittee on Terrorism, Nonproliferation, and Trade on the Committee on Foreign Affairs.* 114th Cong., 2015.

U.S. Congress, *H.R. 2596 Intelligence Authorization Act for Fiscal Year 2016.* 114th Congress, June 17, https://www.congress.gov/bill/114th-congress/house-bill/2596.

Publications

Berger, J.M. "#Unfollow," *Foreign Policy*, February 20, 2013, http://foreignpolicy.com/2013/02/20/unfollow/.

Berger, J.M. and Morgan, Jonathon. *The ISIS Twitter Census.* The Brookings Project on U.S. Relations with the Islamic World, No. 20. March 2015.

Bergen, Peter, "Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment, Hearing before the Senate Committee on Homeland Security & Governmental Affairs," May 7, 2015. http://www.hsgac.senate.gov/hearings/jihad-20-social-media-in-the-next-evolution-of-terrorist-recruitment.

Cohen, Jerad. "Digital Counterinsurgency: How to Marginalize The Islamic State Online," *Foreign Affairs*. November/December 2015.

Dauber, Cori E. “ISIS and the Family Man.” *Small Wars Journal*. July 1, 2015. http://smallwarsjournal.com/jrnl/art/isis-and-the-family-man.

Deardoff, Brad. *The Roots of Our Children’s War: Identity and the War on Terrorism*. Williams, CA: Agile Press, 2013.

Gallily, Yair and Yarchi, Moran. “From Munich to Boston, and from Theater to Social Media: The Evolutionary Landscape of World Sporting Terror.” *Studies in Conflict & Terrorism*, Vol. 38, No. 12 (December 2015): 998-.

Harris, Harris. *@War: The Rise of the Military-Internet Complex.* New York: Houghton Mifflin Harcourt, 2014.

Helluth, Dorle. “Countering *Jihadi* Terrorists and Radicals the French Way.” *Studies in Conflict & Terrorism*, Vol. 38, No. 12 (December 2015): 979-993.

Hussain, Rashad. “A Strategy For Countering Terrorist Propaganda in the Digital Age.” Speech. Australian Countering Violent Extremism Summit Ministerial, Sydney, Australia, June 12, 2015.

Ingram, Haroro J. “Three Traits of the Islamic State’s Information Warfare.” *The RUSI Journal*, Vol. 159, Iss. 6 (December 2014): 4-11.

Klausen, Jytte. “Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq.” *Studies in Conflict & Terrorism*, Vol. 38, No. 1 (December 2015): 1-22.

Morell, Michael. *The Great War of Our Time: The CIA’s Fight Against Terrorism from Al-Qa’ida to ISIS*. New York: Twelve, 2015.

Ohlin, Jens David. *The Assault on International Law*. Oxford University Press: New York, 2015.

Sekulow, Jay. *Rise of ISIS: A Threat we Can’t Ignore*. NewYork: Howard Books, 2014.

Springer Devin R, Regens, James L, and Edger, Edger, David N. *Islamic Radicalism and Global Jihad*. Washington, DC: Georgetown University Press, 2009.

Stakelbeck, Erick. *ISIS Exposed*. Washington, DC: Regnery, 2015.

Stern, Jessica and Berger, J.M. *ISIS: The State of Terror*. New York: HarperCollins, 2015.

Van de Velde, James. “Crash Their Comms,” *The American Interest,* Vol. X, No. 6, July/August 2015, 35-36.

Watts, Clint. “Let Them Rot: The Challenges and Opportunities of Containing rather than Countering the Islamic State.” *Perspectives on Terrorism*, Vol. 9, Iss. 4. (August 2015): 156-162.

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press, 2006.