ONLINE JIHADISM:
PROPAGANDA, RECRUITMENT AND HOMEGROWN RADICALIZATION

by
Gregory Shuck

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
August 2015

© 2015 Gregory Shuck
All Rights Reserved
Abstract: This paper seeks to address current gaps in literature surrounding terrorist use of the internet. The new and rapidly changing nature of the internet, combined with the limited field of research on terrorism studies presents a problem for experts trying to understand these two phenomenon together. Qualitative case studies of terrorist members and groups are examined in order to understand the use of the internet by terrorist organizations and individuals. Results show that the internet has increasingly been used by terrorist organizations to export propaganda, recruit, and radicalize new members. The internet allows terrorist groups and individuals to connect to one another globally, and promote their ideas, networks and propaganda instantaneously across time and space. This negates the physical separation between an organization and a potential recruit, which helps to explain the growing threat of the homegrown attacks in Western countries inspired by jihadist or other organizations abroad.

Chapter one focuses on the academic concept of a lone wolf terrorist, and shows that these individuals are not radicalized within a vacuum, but often interact with other people and media through the internet as part of this process. Chapter two is a comparative study of ISIS and Al-Qaeda’s online recruitment strategies and use of the internet, which highlights the differences between the two organizations and the unprecedented capabilities of the former. The third chapter analyzes ISIS’s social media and online recruitment strategies by looking at the differences between homegrown jihadists and foreign fighters. The new and evolving terrorist use of the internet demands further scholarly research to examine the nature of this threat.

Thesis Advisors: Dr. Mark Stout and Dr. Sarah O’Byrne
Table of Contents

Introduction.............................................................................................................................................1

Chapter 1: Concepts of Lone Wolf Terrorism and Online Radicalization..................................................5

Chapter 2: ISIS and Al-Qaeda Social Media and Online Recruitment.......................................................40

Chapter 3: Theories of Homegrown and Organizational Terrorism in the Age of Global Virtual Communication........................................................................................................................................63

Bibliography...........................................................................................................................................89

Curriculum Vitae......................................................................................................................................100
Introduction

The scholarly field of research concerning terrorism and the internet is relatively small. Following 9/11, research on terrorism increased dramatically as it was considered a much more credible threat than ever before. Although the level of research and academic interest in terrorism has accelerated since that fateful event, it is still a relatively new and limited field of scholarship. At the same time, research on the internet and its various effects has also been limited due to the unique and quickly evolving nature of the world wide web. Our interaction with the internet began in the early 1990s, and has since exploded in scale and capacity, making it difficult for academic work on the subject to keep up. The culmination of these two phenomenon has led to significant gaps in the literature surrounding these subjects, and our overall understanding of the effects of the internet for terrorist groups and individuals.

In this new age of instant virtual communication and interaction, the internet is increasingly capable of connecting geographically separated individuals. The recent explosion of social media platforms has allowed for the emergence of virtual social networks and the sharing of ideas, beliefs and information across the globe. At the same time, the advancement and spread of technology has allowed for increased mobility and access to the internet. Wireless connections and cellular phone capabilities has led to a global increase in the availability and mobility of online interaction. While this has undoubtedly led to a variety of positive effects for our globalized world, it has also allowed for terrorist organizations to utilize these platforms to further their goals.
Groups such as Al-Qaeda have engaged with the internet to promote their ideas and agendas. At the same time, lone wolf and homegrown terrorists have been able to use the internet in their processes of radicalization, as well as the operational aspects of their endeavors. Terrorist organizations such as ISIS represent the culmination of these two phenomena, allowing for the internet to be used both for targeted recruitment as well as the promotion of homegrown radicalization. Although ISIS is presented as the flagship of these abilities through their unprecedented social media campaigns, other terrorist organizations could utilize the internet in similar ways in the future. This is a particularly salient threat given the uniquely fast-paced growth of technology and social platforms available online.

The lack of scholarship and critical research on the conjunction of terrorism and the internet highlights the threat posed by these phenomena, as authorities are uncertain of the effects of terrorist use of the internet. While some scholars tend to emphasize terrorist use of the internet as major and incredibly important threat, others seem to continue to ignore this mechanism as secondary to the kinetic threat posed by terrorism. The truth likely falls somewhere in the middle, demanding a cautious examination of terrorist use of the internet that seeks to understand without overly emphasizing the nature of this threat. This paper seeks to address this gap in the literature and better understand terrorist use of the internet, particularly regarding the use of the internet for recruitment and radicalization.

This paper examines this threat of Jihadist use of the internet and notes several themes. The first chapter addresses a broad base of contested academic theories, such
as the definitions of terrorism and radicalization. It specifically examines the idea of a lone wolf terrorist, and how the internet has demands a reexamination of the term. A “lone” wolf suggests an individual that is a complete loner and in isolation during his period of radicalization and ultimate decision to engage in terrorism. However, chapter one uses several case studies, specifically those of Collen LaRose, Anders Breivik, and Nidal Hassan to show that the internet often allows lone wolves to interact with other individuals and media through the internet during their radicalization, disrupting the classical notion of what constitutes a lone wolf. This chapter serves as a basis for the rest of the paper, which explores the new phenomenon of Jihadist homegrown terrorism inspired by groups such as ISIS and Al-Qaeda utilizing the internet.

The second chapter provides information on the online capabilities and strategies of both ISIS and Al-Qaeda. This comparative study shows the evolution of terrorist use of the internet from Al-Qaeda to ISIS. This study found that ISIS’s social media capabilities far outweigh those of Al-Qaeda or any other known terrorist group, and also highlight their strategies of online recruitment. In order to further understand the implications of social media recruitment by ISIS, literature on commercial use of social media is also examined and compared to the group. The similarities between the business organization’s social media advertisement campaigns and those of a terrorist group such as ISIS are startling. These findings help to set the stage for our final chapter.

Chapter three examines ISIS online recruitment and capability from the perspective of the individuals the organization seeks to recruit. Multiple case studies of ISIS’s recruits are examined in order to gain information on how the group utilizes that
internet to recruit members and disseminate its propaganda. The research shows that there are two categories of potential ISIS recruits, which can be divided into *satellite martyrs* and *foreign fighters*. This dichotomy highlights the two pronged approach of ISIS' recruitment strategy and capability: ISIS seeks to both recruit foreigners to come to Syria and Iraq to join its ranks in person, or to simply launch homegrown attacks of any capacity against people and governments it considers its enemy. Furthermore, its online recruitment efforts seem to be primarily geared toward Westerners, for reasons which will be discussed. This dissertation seeks to further understand the growing importance of terrorist utilization of the internet, particularly that of Jihadist organizations, and the increased threat it poses for homegrown terrorism and recruitment potentiality.
Chapter One: 

Concepts of Lone Wolf Terrorism and Online Radicalization

Introduction

This paper will seek to explore how online media affects the processes of radicalization in individuals, and serves to compel them to engage in acts of lone wolf terrorism. Radicalization has been documented as an incremental part of the process of becoming a terrorist and engaging in politically motivated violence. The internet has exacerbated the trend of lone wolf or homegrown terrorism whereby individuals physically separated from any direct influence by terrorists become virtually indoctrinated and sometimes operationalized. Currently, there are large gaps within the scholarship surrounding online radicalization and its use by terrorist organizations. In particular, the question of whether the internet serves as a primary or secondary role in the radicalization process of homegrown terrorists remains largely unanswered. This paper will seek to address this core issue and others by examining several key case studies.

Multiple case studies will be examined and evaluated based on the actors’ use of the internet. The processes of radicalization in each case will be taken into consideration during these evaluations, as will other variables cited as possible mechanisms of radicalization. How exactly does the internet affect this process of radicalization within lone wolf or homegrown terrorists? It is likely that the internet acts as an accelerator with variable speeds and outcomes. In some cases it serves a primary role, opening a
portal into a world of alternative thinking that gives drive, purpose and a sense of identity to troubled individuals, compelling them to commit acts of violence based on perverted ideologies. In others, it is secondary, functioning as an informational and social nexus that underscores and normalizes radical beliefs already held by an actor, and further enhances his or her motivations to the point of operationalization. It is hypothesized that each case will demonstrate a different level of importance of the internet during the process of radicalization within a spectrum based on the above description.

Literature Review

The literature review section will proceed as follows. First, several definitions will be explored in order to understand the dependent variable of lone wolf terrorism, as well as other key terms. Second, background information on the use of the internet by terrorists and the scholarly debate over important issues within this discourse will be examined. Third, gaps within the current academic field of terrorists’ use of the internet will be addressed in regard to the focus of my paper. Finally, future research will be suggested in order to discern the impact of my work and the possibilities it presents for further studies. It is my hypothesis that, when it is present, online media enhances the
radicalization process of lone wolf terrorists through a variety of mechanisms that are definable and frequently encountered, but case specific.

Terrorism is a difficult concept to define for several reasons. It is often described as a labeling tool that agencies use to legitimate their own agendas. The term “terrorism” remains controversial in the eyes of several scholars. Some of these academics believe that the word “terrorism” becomes a label by which independent individuals automatically associate positive or negative feelings, regardless of context.¹ Bryan, Kelley and Templar go even further, arguing that the term should be abandoned within the academic discourse of political violence as it is inherently “indefinable.”² Other authors take a different approach that allows for the use of the word, while simultaneously considering the negative implications of bias. For example, Richard Jackson argues that although the term has its flaws, it can nonetheless be examined objectively from an “ontological” perspective.³ In his view, there are three mechanisms that must be met in order for an act of political violence to be deemed terrorism: nature, intention and aim.

First, the nature of the act must be “symbolically communicative.”⁴ In other words, it must involve symbolism regarding a particular ideology, religious or otherwise.

² Monaghan et al. 78.
⁴ Jackson, 127.
Second the act of violence must have the intention of communicating a message based on fear, through violence or the threat of violence. Third, the action must be aimed, in some fashion, at a particular political goal. Although this theory may seem too unstructured for any solid analysis of terrorism, it is important nonetheless because its arguments underscore the definition that will be used for the purposes of this study. This study will use the term “terrorism” defined by the US Federal Code of Regulations, which states the definition as “the unlawful use of force and violence against persons of property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.” This definition adheres to Jackson’s theoretical principles pertaining to terrorism. “To intimidate or coerce a government...in furtherance of political or social objectives” through an act of violence highlights all three principles, which posit that the act must be “symbolically communicative” in order to achieve a political goal. More importantly, this definition will allow for our investigation to have structure in the form of government responses and policy implications, ultimately leading to a more substantive discussion.

The second definition that must be agreed upon for the purposes of this study is that of “radicalization.” This term suffers the same controversy as that of terrorism. Authors such as Andrew Hoskins and Ben O’Loughlin posit that radicalization is nothing more than a “myth” supported by particular agencies in order to legitimize their own

---

5 Jackson, 127.  
7 Barnes. See also Jackson, 127.
actions while demonizing their enemies. In a similar approach, Frank Furedi argues that the term “radicalization” simultaneously infers some type of sinister “psychological virus,” while also delegitimizing any reasoning behind the violent action, political or otherwise. Furthermore, Furedi claims that the viewpoint stemming from radicalization is inherently biased, as it is often directed toward Muslim communities. However, Peter Neumann provides a comprehensive explanation of both the process of radicalization and the academic controversy surrounding it.

Peter Neumann argues that the term radicalization is ambiguous, which is why there is much scholarly debate over its use. Despite this controversy, Neumann offers a simplistic approach to the concept of radicalization that also attempts to explain the mechanisms behind its contention. Radicalization is a process whereby an individual becomes extreme. Therefore, radicalization is first and foremost a process of various complexities and variables that ultimately leads to a two part outcome. The first part of this outcome pertains to newly acquired beliefs that are “dramatically opposed to a society’s core values,” or extreme. The second part revolves around the actor’s choice of methods in his or her pursuance of those beliefs or ideologies, i.e. the use of violence regardless of others’ “life, liberty and human rights.” For the purposes of this paper,

subjects will not be considered fully radicalized until they reach the second criteria by carrying out a terrorist act or showing an operational willingness to do so.

Herein lies the debate of what constitutes radicalization. It is difficult to discern between the inception of extremist ideas or beliefs and the actual use of violence to further those ideologies within this process of radicalization. For the purposes of this study, we will take into consideration the fact that different levels of radicalization can occur, while adhering to the singular definition provided by Neumann. However, it should be noted that any actor who meets the first standard but fails the second is not considered fully radicalized. Although they may have begun the process by embracing an alternate ideology deemed illegitimate by society, they should not be considered for these studies until they either carry out a terrorist attack or show signs of complete willingness to do so.

Aside from what actually constitutes radicalization, the exact mechanisms of this process are also highly contested. We have defined radicalization as a two part process, the first of which involves adopting radical or extreme views that are diametrically opposed to the core values of society, particularly in regard to the use of violence. The second step involves actually engaging or attempting to engage in violent or terrorist activity in the name of said ideology. However, how exactly individuals undergo these processes is highly debatable, as such arguments revolve around the uncertain science of understanding how and what a person is thinking.

A few authors give us some idea of how these mechanisms might occur and rework the thought processes and value premiums within a would-be lone wolf. Peter
Olsson describes various authors’ attempts at defining these processes of “thought-
reform,” commonly known as brainwashing.\textsuperscript{13} Singer offers five methods that help us to
understand this process. First, there is an effort to distract the target with exciting,
fantastical, and dramatic experiences, arguments and ideas that keep them from
realizing there is any effort to change or control the individual. Second, time and the
physical environment are both controlled to give the radicalizers a sense of
omnipotence in the eyes of the target subject. Third, the radicalizers attempt to instill a
level of fear or dependency on their target subject in order to achieve total dedication
and obedience. Fourth, old attitudes and beliefs are “suppressed” in favor of new ones
that align with the alternate ideology. Finally, a system of “closed-logic” is put into place
that places an emphasis on framing everything as an “us vs. them” relationship that
highlights and underscores the purported ideology.\textsuperscript{14} Alternatively, Lifton’s model of
radicalization offers five mechanisms of his own that mirror those of Singer’s, while
proposing three more: Doctrine over Person, Sacred Science, and Dispensing of
Existence.\textsuperscript{15} The first of these involves placing the adopted ideology or doctrine of a
group as “center stage” in the life of the target individual. The second refers to the
channeling of any available scientific knowledge in the individual toward the
achievement of operational terrorism, while the final mechanism pertains to the special
status assigned to loyal individuals, particularly martyrs, in the eyes of their adopted

\textsuperscript{13} Olsson, Peter A. 2014. \textit{The making of a homegrown terrorist: brainwashing rebels in search of a cause.}
Santa Barbara: Praeger. 16–18.
\textsuperscript{14} Singer, M. 1995. \textit{Cults in our Midst: The Hidden Menace in Our Everyday Lives.} San Francisco: Jossey-
Bass Publishers, 64-69; See also Olsson 16.
\textsuperscript{15} Lifton, R. 1989. \textit{Thought Reform and the Psychology of Totalism: A Study of “Brain-washing” in China.}
Chapel Hill: University of North Carolina Press. 420-37; See also Olsson 17.
ideological authority. The latter often involves some sort of divine reward.\textsuperscript{16} In our investigation of lone wolves we will look to these “brainwashing” mechanisms as described by Lifton and Singer to determine the precise role of the internet in the process of radicalization laid out by Neumann.

The final term that requires a firm definition before venturing further is the concept of a “lone wolf.” Just as with radicalization, lone wolves can be defined in terms of a spectrum. There are numerous variables that categorize different types of lone wolves. Gabriel Weimann discusses various typologies of lone wolves while adhering to a broader definition that attempts to engage all forms of lone wolf terrorism.\textsuperscript{17} He concurs with the arguments of Spaaij, namely that a lone wolf terrorism must meet the following criteria: “persons who (a) operate individually, (b) do not belong to an organized terrorist group or network, and (c) whose 
*modus operandi* are conceived and directed by the individual without any direct outside command or hierarchy.”\textsuperscript{18}

Segment (b) of this definition will require some adjustment. As will be displayed in the data section, cases vary in terms of the level of interaction lone wolves have with any given network or group of actual terrorists. Several cases will show that this variation in interaction highlights the spectrum of radicalization provided by the internet. While some individuals interact with terrorist leaders or group members strictly through the internet, others eventually meet with them in person, while some never interact with any group element at all. This paper will use Spaaij’s definition while

\textsuperscript{16} Lifton,423; See also Olsson 17.
taking into consideration the various levels of radicalization that each individual lone wolf can experience.

Lone wolves are often discussed in terms of their variability, as they are all different. Some may only become indoctrinated into certain ideologies, while others may become operationally capable. Even within this hierarchy, lone wolves who carry out terrorism in the name of an extremist ideology may choose to engage in different levels of violence. Bates adds to this multi-faceted concept of a lone wolf by positing that there are two overarching types of lone wolves: career and chaos. Weimann explains Bates’ theory. Chaos lone wolves engage in a singular act that is symbolically executed in order to instill a sense of awe in their audience. For example, lone wolves that engage in suicide bombings are often classified as chaos oriented because they are symbolically showing that their cause means more to them than their own life. In contrast, a career minded lone wolf seeks to maximize the level of violence in his actions, thus creating the most significant impact on society within his own reasoning. Other authors add to the discourse of lone wolf typology with their own categorizations. One such is Pantucci, who argues that there are four main types of lone wolves that can be differentiated based on the level of contact that they have with the terrorist group they claim to support. For the purposes of this study, it is important to utilize Spaaij’s

---

set definition of a “lone wolf,” while also taking into consideration the ambiguities of the phenomenon.

Before examining our case studies, we must highlight several themes in the current discourse surrounding the use of the internet by terrorists. Terrorist organizations and individuals have increasingly begun to rely on the internet as a primary tool for advancing their agendas. Authors such as Gilbert Ramsay have elaborated on the various uses of the internet such as information sharing, financing, social and organizational networking, as well as recruitment and radicalization.22 In his case study on right wing terrorists, Chris Hale notes similar findings on the usage of the internet, as well as other uses such as publicity and risk mitigation through encrypted messaging. He also highlights the various ways the internet is used to recruit and radicalize individuals, particularly youths.23 Several authors have explored the variations between individual and group usage of the internet to engage in terrorism.

In their case study of Islamic extremist videos and chat forums, Salem et al. analyze the different ways in which terrorist organizations and individuals engage with the internet. The media from their study focuses on group, individual, operational and non-operational forms of terrorism that target various audiences. Video recordings are particularly significant for their theory as they provide “nonverbal...images of events that can evoke...psychological, emotional... [and] violent reactions.”24 Thus the internet

is used by terrorist groups for a variety of reasons that further their cause. For the purposes of this study, attention will be given primarily to the processes of recruitment and radicalization over the internet.

There are three main categories of thought within the academic discourse of how the internet effects the radicalization process of terrorists. These are communication, training and socialization. The internet is ideal for communication as it allows terrorist groups to reach wider audiences and more thoroughly disseminate information to potential recruits. Other authors go further, such as Paz who argues that Islamic terrorists have begun to use the internet as their main source of information sharing, as it allows for anonymous interaction with a global reach. Lennings et al. add that the anonymity of the internet allows for discourse and debate within terrorist organizations. Terrorist groups utilize the wide-reaching and anonymous communication afforded by the internet for purposes of social networking as well. Neumann posits that online communities of terrorists act as catalysts of radicalization, greatly speeding up the process by encouraging extremist ideology and behavior by normalizing them in a virtual environment. Although communication and

---

social networking seem to be clear motivators for the use of the internet by terrorists, training remains in academic contention.

There are several gaps in the existing literature surrounding terrorists’ use of the internet, one of which is how effective virtual training is in comparison to real world training. A primary example of this debate can be seen in the work of Michael Kenney. He argues that there are two types of training, “metis” and “techne.” The first of these concerns literal experience in the real world, while the latter refers to virtual training. Kenney argues that virtual training does not compare to its real world counter-part, and is therefore not a viable substitute in terms of operational effectiveness. However, authors such as Weimann have given us multiple examples of virtual training and instruction that terrorist organizations utilize, which are easily translatable to real world usage by lone wolves. Indeed, he argues that this is the Al-Qaeda’s new main strategy for attacking foreign targets. My paper will seek to better address these questions using several case studies of my own.

Similar to the debate over online training, another underlying question that remains largely unanswered throughout these studies is how these online processes differ from those same processes in the real world. It is unclear whether online radicalization replaces, enhances or even negates their real world counterparts. However, this debate revolves around another central question, which is whether the internet acts as a primary or secondary factor in its influence over the subject in cases of

30 Weimann, 80-82.
lone wolf radicalization. This study will focus on how these processes of radicalization affect lone wolves through internet usage in comparison with other real-world forms of radicalization.

There remains a considerable amount of academic (and real world) controversy surrounding terms such as “terrorism,” “radicalization,” and “lone wolf.” However, these terms are still broadly used and accepted by a large majority of security analysts, both within the policy world and that of academia. Despite their flaws, it is currently impractical to abandon these terms. Instead, we must take their controversy into consideration and explore the variations of these terms while applying them to real-world cases. This is a major gap in the current academic theory surrounding online terrorism that my paper will seek to address. More specifically, it will examine multiple case studies using the lens of previous academic works in order to produce a study that explores how and why lone wolf terrorists engage with the internet in a variety of ways.

Further research within the field of internet radicalization will also be considered in my paper. In particular, the question of how the online radicalization process occurs will be at the forefront of my investigation. The precise mechanisms of this process have been explored by multiple authors using a variety of case studies. However, there are still gaps in the literature that my paper will seek to answer. More specifically, my paper will focus on the processes of radicalization for lone wolf terrorists. It will attempt to further understand how the content of online media affects the development of radicalization in such individuals. In particular, the question of whether the internet serves a primary or secondary role in the radicalization process remains largely
unanswered. Hopefully, my findings will help to determine the more precise mechanisms of virtual radicalization not only in lone wolf terrorists, but also other violent political actors as well. Along with the contributions of my paper, future research should continue to seek answers to these questions.

**Theory and Hypothesis**

The theories presented above offer a foundation for understanding the use of the internet by terrorist groups and lone wolves. These theories focus on the radicalization of individuals through interaction with online media. There are several gaps within these theories, which my paper will seek to address. As well, a firm understanding of key terms has been highlighted in order for the reader to engage more substantively with the data presented. These theories and rationales will guide this research and help to craft our hypothesis and discussion within the current discourse of online radicalization by lone wolf terrorists.

Despite the utility of these definitions, any contention regarding their meaning should be noted, as it will inherently surround the theoretical analysis of our case studies. Specifically, the notion of a lone wolf will be particularly challenged by our examination. The term ‘lone wolf’ attempts to supplement two loaded concepts, ‘radicalization’ and ‘terrorism,’ with a third arguing that it is possible for a passage to occur from the former to the latter, essentially within a vacuum. This raises multiple questions and uncertainties, especially within the context of the
internet, which can act as a virtual bridge between lone wolves and terrorist sympathizers or operators.

The internet allows for an assortment of interaction and engagement between lone wolves and terrorist organizations. These can include personal messages with terrorist agents or affiliates, exposure to targeted instructional or ideological propaganda, as well as videos, chat rooms, blogs and other media sympathetic to the cause of a terrorist organization. Within these environments, the internet acts in a way described by Jeffry Halverson and Amy Way, as a “contact point,” or “social nexus” that enables virtual interaction between “previously unrelated entities.” These entities can be the potential recruits themselves, or ideologically driven messages and discourse, videos, or even terrorists, their affiliates and sympathizers. The complexity of this social network produces a variety of outcomes through the radicalization of lone wolf terrorists.

Pantucci’s exploration of lone wolf terminology offers a categorical explanation of these outcomes, upon which this paper will build. According to him, lone wolves can be one of four types: loners, lone wolves, lone wolf packs and lone attackers. The first is an individual that carries out a terrorist attack in the name of a terrorist group or ideology, but has had no contact at all with any actual affiliates or members. Lone wolves appear to act completely alone in their process of radicalization and terrorist activity, but in reality they have some tangible contact with actual terrorist agents. Lone wolf packs are the same as lone wolves,

---

32 Pantucci; see also Weimann 78.
except that there are several individuals that radicalize together and engage in subtle interaction with a terrorist organization. Finally, lone attackers are essentially small terrorist cells that have been dispatched by an existing organization. Although they may be or eventually become separated geographically, the actor was already radicalized and part of an existing command structure. This study will exclude the final category using its own criteria, while focusing on a more thorough examination of the differences between the first three and the influences of the internet upon them.

The internet has a variety of effects on the radicalization of lone wolf terrorists in at least a secondary, and often primary role. The main criteria for a primary influence will be the primacy of the internet, both temporally and logistically, during the process of radicalization. For cases to qualify, the internet must be the first medium through which the subject approaches the social nexus described above by Halverson and Way, which enables and encourages radicalization. It must also remain the primary form of interaction between the subject’s chosen ideology or terrorist group. To be considered a secondary factor, the internet must be supplementary to individuals who have already begun to be radicalized by terrorist agents in person. As will soon be discussed in the methods section, cases in which the internet served as a primary mechanism will be the highlight of this thesis.

These case studies are inherently subjective and susceptible to selection bias. All of them have been selected with the prerequisite that they fulfilled the dependent variable, ultimate radicalization and then terrorism. This is due to two factors. First, explanations of the

\[33\] Ibid.
exact mechanisms of radicalization are dispersed throughout various scholarly fields (particularly psychology and social science) the nexus of which is largely stove-piped, controversial, and generally uncertain. Second, there is a concurrent gap in the literature that differentiates between regular internet users and those that become radicalized. Further research should seek to fill this gap by explaining the differences between those who may be exposed to mediums or processes of radicalization, but fail to actually enter its pipeline or follow its track to fruition. However, this academic area is outside the scope of this thesis. It should also be noted that radicalization can occur through similar processes without the use of the internet, however these cases are also outside the scope of this paper. The selection bias will be utilized to thoroughly examine cases where the internet was a clear motivator.

In cases where the internet is primary, it is hypothesized that the internet will act as a type of causal spurious mechanism triggering at least one, if not both steps in the two part process of becoming a lone-wolf. First, radicalization will occur when an individual comes to embrace an extremist ideology and displays a willingness to engage in violence for the sake of said cause. Second, the individual will engage in terrorism in the name of their adopted ideology. It is predicted that the internet will be a significant enabler of these processes. In other words, (z) the internet, will lead to (x) the acceptance and espousal of a radical ideology, often followed by (y) operational terrorism utilizing online interaction. In other words (z) causes (x) and (y); however (z) does not necessarily cause (x) to lead to (y). The (y) variable will likely be more unpredictable as the level and type of interaction online and in person will not only be diverse, but also difficult to deduce from open source material. Furthermore, counter-terrorism interdiction efforts often (and thankfully) disrupt or apprehend subjects before their process of
radicalization is arguably completed (i.e. during the planning phase of a terrorist operation). Although cases in which a terrorist attack is thwarted before it can be carried out would be considered for our study, such failed attacks will not be examined as there is a usually a substantial lack of information on these events. Although these obstacles exist, it is likely that there will still be enough evidence to prove this hypothesis correct.

**Methods**

There are multiple case studies in which the internet was a primary or secondary vehicle of radicalization. However, only cases in which there was substantial use of the internet will be selected in order to form the basis of a fruitful discussion. Thus, individuals such as Jose Padilla will be excluded, as the processes of his radicalization clearly began in the absence of the internet through personal interaction with terrorist agents or sympathizers at home and abroad. Although the internet may have been used as a facilitating mechanism allowing for communication, social networking or possibly training, online interaction was secondary in its effect on radicalization which occurred in person.\textsuperscript{34} Other cases such as Sharif Mobley, a native

\textsuperscript{34} Olsson 47-48, 58.
to New Jersey who somehow became intrigued, enamored and eventually fully radicalized by radical Islamic ideology will also be excluded due to lack of information.

Although it cannot currently be substantiated with solid evidence, it is conceivable that Mobley’s radicalization occurred online as a troubled Muslim youth growing up in a difficult time in America, while struggling to find a sense of identity and purpose. His first reported contact with radical Islamic ideology was his decision to leave New Jersey in 2008 to study Arabic and Islam in Yemen and also meet and become the pupil of Anwar Al-Awlaki.35 Awlaki never met or talked to Mobley before his travels to Yemen, suggesting Mobley began to radicalize through exposure to Awlaki’s messages over the internet. However, there is not enough open source information on Mobley’s use of the internet before and during his process of radicalization. Rather, we will select sources in which the internet can be considered a primary mechanism of radicalization, as discussed in the theory and hypothesis section.

The three cases that will be examined are those of Nidal Hasan, Anders Breivik and Colleen LaRose. We will apply our research question to each of these case studies and evaluate how and why each variable, if any, was triggered by the use of (z) the internet. Our hypothesis will be proven correct in cases during which the internet achieved at least (y) ideological radicalization through communication and social networking, followed by a similar effect on the performance of (x) operational terrorism through virtual training. Our hypothesis will be proven wrong if (z) the internet is shown to have been unimportant or secondary in the attainment of (y) ideological radicalization, or if it is equally irrelevant in the completion of (x) operational terrorism. In other words, our hypothesis seeks to prove the major significance of the internet

35 Olsson 63-64.
within the radicalization process of lone wolves, as it encourages this process through virtual communication and social networking. Furthermore, the internet may be equally significant to lone wolves during the operational phase of their radicalization in which they decide to carry out a terrorist act, as online training supplements their violent fanaticism with logistical capability. Hopefully, these methods within my research will help to determine the effects of the internet on lone wolf radicalization and terrorism.

Data and Analysis

The first case that will be examined is that of Colleen LaRose. Her case study is particularly descriptive of the ways in which online radicalization can occur, as her experience was almost completely over the internet and kept as a secret from her friends, family and live-in boyfriend. Colleen was a middle-aged divorcée living with her boyfriend in rural Pennsylvania from 2004 to 2009. Having previously considered herself Christian, Colleen converted to Islam around 2004, and by 2008 was fully radicalized and engaging in terrorist activity. In 2009 she left the country in an attempt to meet up with online conspirators and assassinate Lars Vilks, the Dutch cartoonist that created a political stir with his cartoon provocatively depicting Mohammad. Prior to her online radicalization and operationalization, her life had been full of cruel and difficult experiences. These included sexually abusive parents,

---

37 Olsson 77.
a lack of an education, substance abuse, minor brushes with the law as well as two failed marriages, the first of which was to a 32 year old when she was 16.\textsuperscript{38} Notably, our other case subjects have suffered similar misfortunes that may predispose them to the effects of radicalization, through the internet or otherwise.

Nonetheless, Colleen only began to radicalize once she became engaged with the social nexus of radical jihadist ideology through the web. This interaction took several forms. Aside from initial learning and conversion to Islam (which is of itself completely benevolent and should not be included as part of the radicalization process), Colleen began to interact with more radical elements of the religion espoused by video postings, blogs and chat rooms that were often vehemently sympathetic to terrorist causes. She often visited websites such as RevolutionMuslim.com, which is used to spread the ideological messages of Shaikh Abdullah al-Faisal, a fanatical cleric that advocates the murder of non-Muslims. She would read postings and articles on this site and others, sharing her own outrage with the US government.\textsuperscript{39} By 2008, she was posting her own video blogs under the username “JihadJane,” often commenting on her dedication to the Muslim world and the cause of suffering Palestinians. She would also refer to non-Muslims as “animals” in 2009, and in a chat room post that same year claim that she was ready to become a “martyr.”\textsuperscript{40} The internet clearly provided a channel of communication for reciprocal ideological rhetoric that encapsulated Colleen, but also further enticed her through the allure of social networking.

\textsuperscript{38} Halverson and Way 140.
\textsuperscript{39} Halverson and Way 143.
\textsuperscript{40} Halverson and Way 143-144.
Colleen’s initial interactions with possible and actual terrorist sympathizers and operators were often through personal messages. Indeed, Colleen seemed to use her new online social environment as a “dating service,” as some sources report she had sustained contact with several Muslim men romantically. In some cases, she would pledge her loyalty to them and their purported jihadist ideology, as well as keep in contact with them for long periods of time. Online social networking supplemented Colleen’s total immersion in her process of ideological radicalization, which can best be illustrated by the figure of her niqab-clad internet avatar.

The images of Colleen in her veiled garb represent her longing to identify with the ideology of her newfound social circle, made even more desirable by a renewed sense of sexual value and prospect. Her niqab or hijab is also symbolic of both her pledge to a new radical interpretation of a faith she probably knew little about, as well as the anonymity the internet provided. It is doubtful that she had more than a basic understanding of Islam considering her lack of education, unfamiliarity with its cultures and languages, and addiction to online video games. Despite her questionable knowledge of Islam, Colleen came to fervently defend and support the radical ideologies of her online community that she primarily (initially only) interacted with through the internet. The question remains whether the internet will remain the focal point of her endeavors in her attempts at operational terrorism.

In terms of training to carry out operational terrorism, the role of the internet is clear in the case of Colleen. Reportedly, by 2008 Colleen began operationally working for unknown terrorist entities intent on waging various forms of radical jihad in Europe and South Asia. According to her indictment, she would “recruit men online to wage violent jihad” in these regions, as well as women for more logistical roles, on the orders of “unknown” electronic communications from various South Asian and Middle Eastern men. She was also instructed to obtain a marriage license in order to smuggle a man into Europe, and advised that her ethnicity (Caucasian) would allow her to go undetected by law enforcement. Throughout the process Colleen repeatedly proclaimed her willingness to become a martyr, and eventually she was given the chance in the form of internet messages that instructed her to meet up with a terrorist cell in Europe to kill Vilks.\textsuperscript{43} LaRose was arrested shortly after her arrival in Europe to carry out her plot, but her intentions and willingness are enough to qualify her as a lone wolf, despite the failure in tradecraft that led to her arrest.

The instructions given to Colleen on what she could do to aid terrorist groups constitute an alternative, even logistical form of training, yet we will evaluate its validity for our hypothesis as acceptable. However, in terms of communication, social networking and arguably even training, the internet was clearly the primary and only source of interaction LaRose had with other terrorist groups during both her ideological and operational stages of radicalization.

The next case study we shall examine is that of Anders Breivik. When exactly the period of radicalization for Breivik began is a point of some contention. From 1999 to 2004, Breivik

worked for the right wing Populist Party and was exposed to their extreme views on immigration policy.\textsuperscript{44} However, his radicalization did not actually begin until his subsequent engagement with online discourse advocating violence in the name of radical ideology. Although he began believing in radical ideas supported by the Populist Party, this is the first clear evidence that he advocated violent activity in the name of these ideas. Like Colleen, Anders had a troubled childhood before his eventual transformation to a lone wolf terrorist, including poor parental guidance through the lack of a father and an unstable mother.\textsuperscript{45} Furthermore, Breivik was a member of several petty gangs as a teenager that would engage in low-level crime such as graffiti.\textsuperscript{46} But his online radicalization began with his engagement of right-wing radical ideology over the internet, using the alias “Morg” to join the discourse of blogs, forums and chat rooms.\textsuperscript{47} The period of 1994 to 2004 saw the beginning of this interaction that laid a solid foundation for Breivik’s continued radicalization through communication and social networking.

After 2004, he increasingly interacted with terrorist sympathizers and supporters through websites such as Gates of Vienna, Stormfront and Nordisk. These are all radical right-wing forums which surrounded him with an interactive social and ideological atmosphere of racism and Islamaphobia, allowing him to channel his rage at an identifiable source of ‘us’ vs. ‘them’ elicited by the nature of such beliefs.\textsuperscript{48} It should be noted, that although there is no

\textsuperscript{44} Feldman, M. 2012. “Viewpoint: Killer Breivik’s links with far right.” BBC News, August 27.
\textsuperscript{46} Borchgrevink 60-62.
\textsuperscript{47} Borchgrevink 122.
acute evidence of Breivik associating directly with any terrorist group through the internet, he likely unknowingly engaged right-wing terrorist sympathizers, supporters, or possibly even agents. The limited research on right-wing lone wolves suggests a recent rise in the number of small groups and individuals that engage in terrorist activity, particularly “lower level acts of violence, which cumulatively are having a serious impact on communities across Europe but are less likely to make the national headlines.”

While they may not have given him direct instruction or training, they more than likely encouraged the use of violence in the name of their ideological cause.

Breivik continued to utilize the internet during his process of radicalization. However, the level of training provided by the internet for Breivik’s terrorist act is more uncertain. In 2006, Anders moved back in with his mother “to save money and play video games.” While this turned out to be true, Breivik also used this time to continue his online radicalization through interaction with other right-wing extremists and to write his compendium, a manifesto pronouncing his radical beliefs that turned out to be nothing more than an assortment of plagiarized counter-jihadist rhetoric. This period of radicalization was intensified by long periods of isolation, multiple failed business attempts, and hours of video games. In 2010, Breivik began logistically preparing for his attack by using the internet to procure and assemble

---


50 Borchgrevink 138.


an array of small arms, ammunition, body armor material and fertilizer bombs.\textsuperscript{53} It is clear from these facts that the internet played a primary role in at least a communicative and social capacity, for fomenting the radicalized beliefs of Breivik. It is unclear how much training or instruction Breivik received through the internet, but at the very least it was used in a logistical fashion to facilitate the procurement of arms and material for his act of terrorism.

The case of Nidal Malik Hasan is more ambiguous in terms of the utility of the internet within the context of radicalization. Hasan, a middle-aged Muslim American of Jordanian descent was serving as a doctor in the US army in 2009, when he decided to carry out a terrorist attack against his fellow soldiers, leaving 13 dead. Having shown clear signs of experiencing an identity crisis in the midst of his controversial Muslim views and his profession within the US Army, Hasan’s ideological anxiety went into overdrive and triggered an act of terrorism three months away from his expected deployment to Afghanistan.\textsuperscript{54} The internet seems to have been used by Hasan as a facilitator in his process of radicalization. Unlike the other cases, Hasan had direct contact with a terrorist organization through the internet from the beginning of his radicalization. Hasan contacted Al-Qaeda propagandist Anwar Al-Awlaki, and emailed him around 20 messages from 2008 to 2009.\textsuperscript{55} However, experts that have examined the emails note there was nothing incriminating about the messages, suggesting Awlaki did not directly prompt Hasan to carry out the attack.\textsuperscript{56}

\textsuperscript{53} Borchgrevink 141-142.  
\textsuperscript{54} Olsson 50-53.  
\textsuperscript{55} Olsson 51.  
\textsuperscript{56} Olsson 52.
The communication between Hasan and Awlaki was extremely one sided. Several of Hasan’s emails with Awlaki were intercepted and cleared as non-threatening by an FBI investigation that began in December, 2008. In fact, Awlaki had not even responded to any of Hasan’s messages by the time of the conclusion of the investigation in June 2009.\(^57\) Then in November, Hasan carried out his attack. Based on the lack of involvement by Awlaki in their conversations, it is conceivable that their relationship was largely one of idolization by Hasan. Hasan showed great interest in Awlaki’s teachings and emailed the preacher numerous times. He even offered his assistance in any way and gave Awlaki his contact information in case he might “find [him] useful.”\(^58\) It is unclear from solely open source information whether Awlaki and Hasan had any further contact, through email or otherwise, that would place a higher premium on the internet as a facilitator of radicalization. However, at the very least it is clear the internet served as a secondary function whereby the subject could entertain his thoughts of radical ideology or terrorism in the virtual presence of an idolized individual who vehemently supported those very ideas and processes.

During this online interaction, Hasan sent all of the messages and Awlaki never responded. This suggests the internet acted in a secondary capacity by allowing Hasan to channel his previously held beliefs to an even higher level of devotion that may have helped push him toward completing his radicalization and engaging in operational terrorism. However,

\(^{58}\) Ibid.
this is merely speculation and the case of Nidal Hasan clearly lacks any solid evidence that points to the internet as a primary actor.

Despite the lack of concrete evidence showing a process of radicalization caused by the online interaction of Hasan and Awlaki, the contents of these messages may help us understand how Nidal began to justify acts of terrorism in the name of extreme ideology. In an email in May of 2009 to Awlaki, Hasan defends suicide terrorism and justifies its use through a story. In it he describes the permissibility of suicide bombing, as long as the intention of the perpetrator is sound. Should a soldier sneak into a camp and detonate a suicide vest to stop future attacks on his comrades, this would be justifiable, Hasan argued. Although Awlaki never responded to this email, we can see how Hasan began to grow emboldened by the idea of operational terrorism in the virtual presence of his idol. However, there is no clear evidence that Hasan received direct influences of radicalization through the internet. Thus, the internet was secondary in the case of Nidal.

Nidal’s radicalization seemed to have already begun even before his interaction with Awlaki. He began showing signs of a firm belief in radical ideologies as early as his residency, yet it is unclear whether he used the internet as vehicle for these beliefs. There were multiple signs of his radicalization during his time in the Army as well, suggesting that Hasan’s radicalization was in place prior to his interaction with Awlaki. Hasan’s sanity was also questionable, as his psychiatrist colleagues would use terms such as “paranoid,” and “schizoid,” to describe his mental state. Notably, Hasan lacked several of the predispositions to radicalization that the

---

59 Ibid.
60 Olsson 50.
other two case studies experienced, such as a traumatic childhood, severe lack of education and previous engagement in petty crime. We will explore this cross-examination further in our discussion, as it could explain why Breivik and LaRose were so susceptible to the internet as a primary motivator as opposed to Hasan.

Two out of three cases proved our hypothesis, while a third was too ambiguous to qualify. Anders Breivik and Colleen LaRose became ideologically radicalized primarily through their online interactions, which then continued to fuel their radicalization process to the point of operational terrorism. Clearly in the case of LaRose, and arguably Breivik as well, the internet played an equally significant role in radicalization through communication, social networking and training. With these outcomes, our hypothesis has several implication for future research.

With the exception of Nidal Hasan, the cases above show us that the internet should indeed be considered a possible primary mechanism in the causation of ideological radicalization, and even operational terrorism, within lone wolf subjects. For these cases, it is clear that the internet acted as a catalyst for troubled individuals to gain acceptance within an online ideological circle of identity, provided by a virtual social and informational nexus. In the case of LaRose and Breivik, it was shown that they may have fundamentally misunderstood the very ideologies they claimed to uphold. LaRose’s poor education and limited exposure to Islam may seem more pronounced, however Breivik’s entire compendium, which he developed throughout his years of radicalization turned out to be a hollow collage of plagiarized pieces written by right-wing fear mongers.61 These predispositions of LaRose and Breivik, which were

---

61 Halverson and Way 142; see also Shane (2011).
lacking in the case of Hasan, may have enabled the internet to fulfill such a prominent role in their radicalization.

It is conceivable that these conditions may have accelerated their tenacity in seeking acceptance, and the rapidity with which they became indoctrinated and prepared to commit violence in the name of a radical ideology. This concept has important implications for future scholarship on radicalization, as it suggests the internet allows for the spread of extreme ideological discourse that supports violence, to which lone wolves can adhere without having to understand or be persuaded by the actual arguments of said discourse. In other words, lone wolves that rely primarily on the internet for their process of radicalization are able to engage with terrorist groups or activity with little actual knowledge of the ideology they claim is driving them. This is a crucial point that demands more exploration.

By showing that the internet can be a significant motivator in lone-wolf terrorists, we can understand some of the confusion and debate surrounding the exact motivation for radicalization. As has been explained, the internet allows for synergy between two entities previously unconnected and within their own separated physical vacuums. Before the internet, this type of interaction was not possible and the transplantation of radical and foreign ideas from one part of the globe to another in such a fast and dramatically violent manner was unheard of. Today, this process is not only possible, but also capable of further enhancing itself through the quick-paced evolution of the internet. Let us remember that the internet has only been relevant (the form of major accessibility) for the past two decades. It should also be noted that our two unique cases of Breivik and LaRose becoming radicalized and operational completely online were within the past 5 years. As the internet has grown, new technologies
and improved logistics have allowed for extensive increases in the speed, range, availability and type of online interaction throughout the globe. It is speculation, but these two cases may be early examples of a phenomenon that will continue into the future. The internet will continue to expand and innovate in ways we cannot even predict, suggesting that physical distance will become less and less relevant in a world increasingly interconnected through virtual reality. The case studies we examined may prove helpful in deciphering the process of radicalization in lone wolves, particularly in light of their relatively new and unique online experiences.

The ways in which the subjects of our case studies interacted with their respective online media demands a reexamination of our definition of lone wolves. Indeed, all three segments of our definition supplied by Spaaij are uncertain in the light of our case studies. How can a lone wolf be someone who “(a) operate[s] individually, (b) do[es] not belong to an organized terrorist group or network, and (c) whose modus operandi [is] conceived and directed by the individual without any direct outside command or hierarchy,” if the internet affords the actor alternative forms of interaction with terrorist ideologies, sympathizers, agents and groups? Subjects such as Breivik and LaRose are considered two classic examples of lone wolves, yet their extensive use of the internet as a vehicle of their own radicalization challenges the notion that they operate completely alone and never come into contact with actual terrorist groups or networks. They may physically live within a vacuum in regards to their chosen radical ideology, but they also engage in a variety of virtual connections and interactions.

62 Spaaij.
interactions. Perhaps a new definition of lone wolves should be considered, more in tune with Pantucci’s categorical approach.

It is noteworthy that there are cases in which the internet was clearly a primary motivator, such as Breivik and LaRose, and that there are others in which the internet was either secondary or unimportant. With Breivik and LaRose, our hypothesis was proved entirely correct, as (z) the internet was clearly a primary cause of (x) radicalization and also (y) operational terrorism. However, the case of Nidal Hasan was different. A third category may be necessary in light of Hasan’s case, which showed us that lone wolves can utilize the internet in more ambiguous ways, such as personal messages with an Al-Qaeda recruiter that lack any concrete evidence of terrorist collusion, but will remain somewhere along an elusive spectrum between direct causation and pure coincidence. Indeed, it remains unclear what effects the internet had on Hasan, despite its facilitation of his interaction with his idol, Awlaki, which was certainly of relevance. But this only seemed to cement beliefs that were already clearly held by Nidal long before his notorious emails were ever sent. Perhaps we can describe the internet as a strong secondary influence during the final stages of his radicalization, which helped him take his final steps and ultimately engage in operational terrorism. This is particularly convincing given the content of his messages (justifying martyrdom), their recipient (a known Al-Qaeda propagandist), and their timing (in the months leading up to his attack). This case may merely be a subset of the initial indications that the internet was secondary as according to the methodology and framework of this study, but it showed strong potential as a motivation to cause (z) to lead to (y) alone. Finally, it is important to remember that these case studies were inherently subject to selection bias.
As noted in the theory and hypothesis section, our case studies were intentionally selective in order to examine cases in which the dependent variables were triggered. Cases in which internet users engaged with materials, individuals, websites, games or other media associated with radical ideology or terrorism were not reviewed because their sheer volume alone is outside the scope of this paper. Furthermore, such large case-n studies that examine the issue from a macro level of comparison between lone wolves and regular internet users are few in the field of online radicalization. This is a critical gap in the current academic discourse of lone wolf terrorism that should be addressed with future research. Nonetheless, all of our findings and the concepts expounded upon above could have important implications for future counter-terrorism research and policy.

As we have seen, it is difficult to conduct accurate scholarly analysis of these cases with the limited availability of open source material. Secrecy surrounds many of these case subjects and their processes of radicalization, particularly online. This is undoubtedly an important dynamic of counter-terrorism efforts, but perhaps some type of additional transparency should be considered for the purposes of more thorough scholarly investigation. Without the aid of academic research, counter-terrorism analysts will be hindered in their capacity to completely understand and foresee the threats posed by lone wolf radicalization over the internet. Although we are not privy to their exact methods, counter-terrorism officials have clearly detected the importance of online radicalization as they were able to apprehend Miss LaRose. However, misunderstandings still exist, as the attacks of Nidal Hasan could have clearly been thwarted given the red flags of his internet use. This paper has hopefully addressed some of that misunderstanding by demonstrating that the internet can act as a virtual vortex of
information and influence that acts as a primary or secondary mechanism in the radicalization of lone wolves.

**Conclusion**

This paper has sought to explore the phenomenon of lone wolf terrorism through the relatively young and hotly contentious academic field of online radicalization. The literature review gave a brief overview of the scholarship surrounding key terms, and selected specific definitions for use within our thesis question and hypothesis. Attention was given to selective arguments that highlighted the general debate over these terms and their implications for our analysis. Theoretical debate surrounding the complexity of connecting contentious processes and concepts, such as terrorism, radicalization and lone wolves helped us to build a framework for the mechanisms of our hypothesis. The methods of our research were limited by a general lack of case studies and open source information on specific data, particularly in relation to internet usage. However, we were able to examine several case studies that triggered the variables in our hypothesis, which yielded intriguing results.

It is clear that in some instances of lone wolf terrorism, the internet can play a crucial role throughout the entire process of radicalization, up to and including the potentiality of operational terrorism. Within the context of this argument, we must remember that the existing body of scholarship dedicated to the online radicalization of lone wolves is still
extremely new and small. Hopefully this work will help to assert the significance of the internet as a primary facilitator for the radicalization of lone wolf terrorists.

In particular, the cases of Anders Breivik and Colleen LaRose have shown us that the internet can act as one of the most and even only sources of radicalization in lone wolf terrorists. The unique and similar nature of these two cases deserves further analysis, particularly in light of the role of the internet. Nidal Hasan used the internet in a secondary capacity, although we have discussed its strong influences and its possible connections to his terrorist attack. The internet can indeed be a significant motivator in lone wolf attacks, and the lack of academic analysis on this medium of radicalization warrants further research on the topic. However, it is clear from the findings of this study that the internet can be primary, secondary, or even crucially secondary in the process of radicalization in lone wolf terrorists.
Chapter Two: 
ISIS and Al-Qaeda Social Media and Online Recruitment

Introduction

Social media is a new online phenomenon that allows organizations to quickly and effectively engage a target audience. Businesses have discovered this new tool and are rapidly working to understand and enhance their own social media capabilities. Social media is often used by the commercial world to advertise and sell products to the public through intense personal interaction and engagement. Politicians have also found this new media wave inescapable, as every US senator and nearly every Congressman now find themselves operating a Twitter account to interact with the public.63 This media has allowed for real-time relations between an entity and its constituent or customer, which are used to communicate ideas, actions and justifications.

Similarly, terrorist organizations have also begun to utilize this form of online media to achieve their goals and reach potential recruits. Although not all terrorist groups have been willing or able to embrace this virtual vehicle of ideology, some have been able to master the nuances of social media, and the effects of their efforts are truly alarming. This chapter examines two case studies, ISIS and Al-Qaeda, to determine how these organizations utilize social media and the internet to further their goals and gain new recruits.

ISIS has an incredibly sophisticated online propaganda machine that uses a vast array of tools to conduct recruitment. Internet social media is the weapon of choice for ISIS. These cyber-recruitment campaign targets individuals to either join ISIS in the Middle East, or wage jihad from home.\textsuperscript{64} While these smaller homegrown attacks will continue to remain the primary threat to Western countries, in the longer term the numbers of Westerners that travel to join ISIS in person will also continue to increase. Of course, the threat such recruitment poses to regional Middle Eastern countries is all too evident in the past successes and territorial gains of ISIS. Although it uses this media to recruit people from Middle Eastern countries as well, the complete freedom of movement afforded Western internet users has made them ideal targets for the organization. Al-Qaeda also uses the internet to further its goals and gain new followers, but they operate online in a different way.

Al-Qaeda uses the internet to reach potential recruits as well, and often finds itself in competition with ISIS over the same pool of candidates. Rather than primarily rely on social media to deliver their messages and engage current and potential members, Al-Qaeda projects traditional forms of media over the internet.\textsuperscript{65} To truly understand the difference between these organizations and their use of social media (or lack thereof), we will discuss the literature surrounding the commercial use of social media. Through comparison, these theories of marketing and advertisement will help us build a framework for understanding how terrorist


groups such as ISIS and Al-Qaeda utilize social media for the purposes of enticing a particular audience.

**Literature Review**

Traditional online media existed before the prevalent use of social media. These include text, videos and audio recordings that are often found on webpages. Although social media employs these same forms of media, the key distinction between traditional media and social media, is that the latter employs the former to engage and inform individuals based on community interaction. Social media is described by Kaplan as “virtual worlds,” within which individuals can interact with one another, creating their own “collaborative projects... [and] content communities.” Haythornthwaite notes that social media sites reinforce preexisting social networks that have variable degrees of interaction offline as well. At the same time, this offline interaction ensures that the ties of the group or community utilizing a social media site stay strong. Boyd and Ellison provide a more structured definition of social media:

> Services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection,

---


and (3) view and traverse their list of connections and those made by others within the system.\textsuperscript{69}

This definition is used for this paper because it allows for a firm understanding of social media despite its inherently dynamic nature. In other words, this definition can be applied across the various forms social media platforms and interactions. This definition is most applicable for an analysis of terrorist group marketing strategies and theories of social media utilization.

Businesses have come to realize the potential of social media networks for the purposes of marketing and advertisement. One of the main themes of social media relations between companies and customers pertains to interaction. Many studies have confirmed that the special and unique aspect of social media allows for a virtual conversation between a particular business and its patrons.\textsuperscript{70} Before the existence of social media, companies primarily used push-marketing strategies that simply dumped messages and information in the laps of consumers. Social media allows for an alternative pull-marketing approach that thoroughly engages the consumer and allows him or her to ask questions and interactively learn about a brand.\textsuperscript{71} The proper distinction between push- and pull-marketing turns “broadcasts... into

\begin{itemize}
\item \textsuperscript{69} Boyd, Danah M. and Nicole Ellison. “Social Network Sites: Definition, History and Scholarship.”\textit{Journal of Computer-Mediated Communication,} vol. 13, no. 1, October 2007. p. 211.
\end{itemize}
Thus, the traditional relationship between the consumer and the company in marketing strategy has been radically altered through the use of social media.

There are several factors within these virtual conversations that demand closer examination. It is noted by multiple authors that this interactive conversation empowers the consumer due to its voluntary nature. Evans explains that this relationship demands a higher degree of trust between the advertiser and his audience, but it also leads to greater brand loyalty once a trusted relationship has been firmly established. Gunelius confirms this view, and adds that the process of “building relationships” has been given a higher priority than ever before in social media marketing strategies. Finally, these online communities and relationships nurtured through social media are increasingly becoming available on mobile platforms such as smart phones. This allows marketers to reach clients virtually at any time and any place throughout the globe. The virtual conversation provided by social media platforms empowers its clients through voluntary and personal interaction. This in turn leads to a firmer and more trusting relationship between companies and their customers, but forces businesses to place a higher premium on accountability than they ever have before.

Aside from the interactive and conversational aspects of social media interaction, there is also a higher standard of qualitative demand. However, there is some contention among authors regarding the cost-benefit analysis of using social media marketing strategies. Funk argues that the rewards from social media advertising can be powerful, but companies must

72 Anand 3.
73 Evans 30-31.
74 Gunelius 3.
75 Kaplan 129.
invest heavily in social media experts that can target audiences using sleek and highly refined campaigns. This requires considerable financial resources and human capital. Others claim that although substantial investment is required for a successful social media strategy, the benefits far outweigh the costs. In fact, they argue that costs are inherently decreased by using social media marketing. Decision-making becomes more decentralized and marketing efforts are virtually outsourced to consumers within their social media communities, a strategy known as “crowd-sourcing.” The cost-benefit debate between these authors raise important points for our study.

Social media marketing can create stronger relationships between a company and its consumers. However, in order to ensure success, a high degree of time, money and effort must be invested in social media marketing strategies. Although social media can decrease costs and increase consumer loyalty, the inherent weakness or danger of this approach is that a certain level of control over the marketing campaign is redirected from the company to the consumer. This can become a major problem not only for business, but also politicians and even terrorist organizations that employ similar social media marketing strategies.

Politicians and their public relations teams have also begun to tap into the world of social media and reap its many rewards. Scholars have noted that senators and congressman have increasingly begun to use their own social media accounts to interact with their

---

77 Anand 7; Macy and Thompson 83.
79 Anand 7.
constituents. There are several impacts of this phenomenon. Notably, this interaction is different from previous communication between politicians and those they represent because it is both free and almost instantaneous. \(^{80}\) Furthermore, social media is “transparent” and can be easily studied to determine the effects of such cheap and immediate interaction between politicians and their constituents. \(^{81}\) This allows social scientists the ability to study this interaction thoroughly and discover its impacts. Researchers can similarly apply these concepts to their study of terrorist organizations’ use of social media.

There is currently a significant lack of literature concerning theoretical approaches to terrorist use of social media. Some of the lack of literature is because social media is a recent phenomenon (terrorist use of social media is even more unfamiliar), as well as the clandestine nature of terrorist activity. However, the work of J.M. Berger allows us to understand several aspects of terrorist organizations use of social media.

Berger gives us a general view of how terrorists utilize social media. Terror groups employ social media to amplify their messages and exponentially increase the impact of their goals. \(^{82}\) These goals can include anything from recruitment, ideological legitimization, or simply fear mongering. However, the larger point is that the use of social media allows small terrorist groups to disproportionally increase the range of their propaganda. At the same time, terrorists have also begun using cyber tactics to enhance their social media exploits. \(^{83}\) These include

---

\(^{80}\) Straus et al 2.

\(^{81}\) Straus et al 3.


\(^{83}\) Ibid.
methods such as Twitter-bots (machine generated Twitter accounts) and “hashtag-bombs,” which subversively redirect users from a popular hashtag to a terrorist video or website.  

A third general aspect of terrorist use of social media is their abuse of unrestricted Western web access. Terrorist organizations take advantage of the absolute freedom of movement within Western internet environments. This suggests that Westerns are the primary targets of online social media recruitment. However, Western countries have recently begun cracking down on terrorist group activities within their web.

While social media and terrorist use of such platforms is still in its infancy, an even newer environment of online suppression of these activities appears to be emerging. Berger notes several aspects of this new era. First, the goals of terrorist organizations are obviously harder to achieve through the use of social media as their activities are now being stifled. Second, the retention of certain accounts and users (it is unclear if this is purposeful or not) by terrorist groups allows law enforcement and military agencies the ability to track and monitor terrorists and their affiliates. Third, specific accounts and users that are hyper-active within the spheres of terrorist social media can be targeted and eliminated, further hampering the efforts of terrorist groups over the internet. It is too early to concretely pinpoint the effectiveness of these countermeasures in the fight against terrorism, however there are several areas of concern that can be identified.

---


85 Berger.

86 Berger.
Berger notes that three issues remain a concern and garner contention within the counter-terrorist discourse regarding social media. These revolve around transparency, consistency, and scope. Transparency is important to Western countries that cherish their rights of privacy and freedoms of expression. The balance between respecting these rights and ensuring the security of citizens will continue to be a critical aspect of countering terrorist organizations’ use of social media and the internet. Consistency will also remain a crucial factor, as some internet providers or social media companies may be more cooperative than others in the fight against online violent extremism. Finally, Berger argues that we must ensure proper perspective within the scope of social media threats. Aside from terrorism, state-sponsored attacks and other forms of social media abuse, such as personal harassment, must also be taken into consideration. Along with commercial marketing theories, these aspects of terrorist use of social media will be used in our comparative analysis of ISIS and Al-Qaeda.

Methodology

This paper uses the literature on social media described above to analyze ISIS and Al-Qaeda’s internet recruitment strategies. In our comparison, special attention is given to the

87 Ibid.
88 Ibid.
ways in which Al-Qaeda and ISIS engage in marketing strategies and themes that are similarly used in the commercial world. There are several aspects of social media marketing that we can extrapolate and test within the marketing systems of terrorist organizations. Social media platforms are interactive, community oriented and experienced in real-time across a variety of free to use websites and cellular phone programs. These aspects of social media demand large-scale organizations to operate their own social media offices that can help to guide the free flowing conversations between themselves and their customer base. Major investment in such operations and marketing campaigns is a necessity for staying on top of the powerful but unpredictable nature of social media advertisement. Our case studies will show how terrorist organizations mimic these social media marketing strategies through their own online recruitment. It is hypothesized that both groups utilize social media as a primary tool for online recruitment, however ISIS’s capabilities far exceed those of Al-Qaeda.

Data and Analysis

Al-Qaeda has traditionally relied upon several individuals and organizations to create and disseminate its propaganda. The terrorist group uses a massive media wing known as as-Sahab, which “produces documentary-quality films, iPod files and cellphone videos.”90 These videos created by Al-Qaeda’s media wing began to grow exponentially in the mid-2000s. In 2002, only 6 videos were produced throughout the entire year, but in 2007 this number increased to 97. However, this activity has seemed to decline at least qualitatively in more recent years. In 2014, as-Sahab released an old video from 2000 of the bombing of the USS Cole along with a recording of the group’s deceased leader Osama bin Laden.91 Nevertheless, this type of media that focuses on the messages and directives of Al-Qaeda’s leaders is consistent with the traditions of the group’s online propaganda efforts.

The leadership of Al-Qaeda is often at the forefront of the group’s propaganda efforts. Leaders such as Osama bin Laden, Ayman al Zawahiri and Anwar al-Awlaki propagate their own teachings as the official ideological beliefs of Al-Qaeda, disseminating these ideas to their recruits and members hierarchically.92 Al-Qaeda uses a variety of media forms as vehicles for the messages of their leadership, including YouTube videos, online blogs and forums, as well as the infamous Inspire magazine, a digitally available jihadist magazine founded by Awlaki and

produced by Al-Qaeda.\textsuperscript{93} However, Al-Qaeda’s leadership also interacts personally with many of its members and potential recruits through the internet. Awlaki has personally had contact through email and instant messaging with multiple individuals seeking to join Al-Qaeda or carry out terrorist attacks on its behalf, such as the Fort Hood shooter Nidal Hassan.\textsuperscript{94} Other leaders such as Zawahiri have hosted public forums online where anyone can ask any question and Zawahiri himself would respond. An estimated 2,000 queries were asked of Zawahiri in December of 2007, who answered around a fifth of them giving justifications such as the killing of any Egyptian police officer for being “infidels.”\textsuperscript{95} This type of direct contact between the hierarchical leadership and lower level members of the organization seems to be a trait specific to Al-Qaeda rather than ISIS.

Al-Qaeda has recently begun to shift its propaganda efforts from strictly using traditional forms of online interaction, primarily jihadist websites, to social media platforms. In the past, Al-Qaeda relied heavily upon jihadist websites that could be found primarily in English or Arabic, and which included chat forums, video archives, audio recordings, and other traditional online media. They would often be somewhat difficult to enter, sometimes requiring users to register with a username and password in order to give the sites a foundation of privacy.\textsuperscript{96} Websites such as Shamukh al-Islam offered jihadists a virtual environment to

\begin{itemize}
  \item \textsuperscript{95} Whitlock.
\end{itemize}
communicate and digest media produced and disseminated by Al-Qaeda leadership and its members. However, this website, like many others, was recently shut down by authorities in 2012. As a result of these efforts by law enforcement and government entities, and possibly in an attempt to keep up with its ISIS counter-part, Al-Qaeda has begun to increasingly rely upon social media platforms such as Facebook and Twitter to disseminate its online propaganda. In contrast, ISIS itself was born within this new age of social media, and has immediately adopted social media as the main engine for its propaganda machine.

ISIS operates several different organizations under its media wing, which help to perpetuate its message and amplify it over the internet on a global scale. In 2006, one of ISIS’s main predecessor groups formed al Furqan Institute for high-quality media production to be distributed through DVDs, CDs, and online material, which ISIS still uses today. In 2013 another media branch was set up by ISIS under the name of I’tisaam Media Foundation in order to produce jihadist propaganda, however this particular site was shut down by Twitter in June of 2014. ISIS uses a multitude of these jihadist sites, which feed of one another and replicate the same ideological online environment ideal for radicalization. ISIS also operates its own social media application originally created by Palestinian militants known as “The Dawn,” which uses computer code to piggyback onto Twitter networks while bypassing anti-spam filters.

97 Clayton.
The group uses these online platforms to promote its narratives, solidify its basis of support, intimidate enemies and recruit new members.

The reach of the internet allows ISIS to focus its propaganda efforts not just within the Middle East but also throughout the globe. The main organization responsible for targeting Westerners for ISIS recruitment is called Al-Hayat Media Center, which was established in July of 2014. It translates other ISIS material into English, German, Russian and French while also producing its own original content focused specifically on recruiting Westerners.\(^{100}\) There is other evidence such as eyewitness testimony and analysis of social media, which strongly suggests that ISIS is purposefully targeting Westerners as highly valuable potential members. At least 2,000 Westerners have travelled to Syria and Iraq and may now fight for ISIS, although some of those could be fighting for one of the several other smaller jihadist factions.\(^{101}\) These recruits come from Western nations around the world, including an estimated 50 from Spain, 100 from Canada, 100 from the US, 130 from the Netherlands, 200 from Australia, 250 from Belgium, 320 from Germany, 400 from UK and 700 From France.\(^{102}\) ISIS has also recently begun using its propaganda machine to influence Westerners via the internet, and convincing them to conduct terrorist attacks on their own soil. In September 2014 (in response to US coalition airstrikes) an ISIS spokesperson, Abu Mohammad al Adnani, released a 42-minute video calling for homegrown attacks against the US and its Western coalition allies. Suggested attacks


included bombing, shooting, or assaulting by any means Western citizens or military personnel who are “disbelievers.”

The ISIS media branch is led by Abu Amr al Shami, as well as Abu Mohammad al Adnani. The former, al Shami, is responsible for the proliferation of ISIS media and ideology. He operates an extensive underground network of online hackers, writers, researchers and bloggers to help him disseminate ISIS propaganda material globally through the virtual superhighway of the internet. The most prolific and tech-savvy cyber jihadists are not only dedicated but also incredibly talented, not only at creating propaganda but also more importantly at physically manipulating computer networks and systems to disseminate this information to larger social media networks. This core of cyber jihadists, sometimes called the “media mujahidin,” are a new breed of terrorist that has not been seen to this extent within the context of Al-Qaeda’s online propaganda efforts. Although this cadre of hardcore believers acts as the main muscle in propagating ISIS material online, social media platforms are used by the group to quickly disseminate and circulate this information to their followers and potential recruits.

Cyber jihadists also use computer code to amplify their ideological message throughout the internet, avoiding detection and censorship by the authorities. ISIS internet lackeys spread throughout the world monitor social media and use tools such as Twitter bots (machine generated twitter accounts) and Twitter bombs to hijack popular hashtags and redirect

---


unaware Twitter users to ISIS propaganda through malicious computer code.\textsuperscript{105} Aside from utilizing Twitter, Facebook, YouTube, Instagram and its own social media applications to promote its pictures, videos and other forms of propaganda, ISIS has even claimed to have begun work on its own Grand Theft Auto-styled video game.\textsuperscript{106} The leadership of al Shami and the work of his tech-network provide the backbone for ISIS’s propaganda efforts.\textsuperscript{107} However, the massive online community of ISIS supporters using social media constitutes the rest of the body for ISIS’s propaganda efforts.

It is important to note that ISIS uses social media to virtually “crowdsource” its propaganda efforts. Although ISIS media operations have leaders such as al Shami and spokespeople such as al Adnani, the real threat is the ability of ISIS to outsource (or, “crowdsource”) its propaganda efforts to its followers. Twitter, Facebook and other social media platforms allow users to tap into a general theme of ISIS ideology while adding their own unique views, experiences and perspectives.\textsuperscript{108} ISIS does not need to rely on the charisma of a central leader to dictate ideology to its membership because its members can now do that themselves collectively and instantly using technology and the internet. Although the group’s

\begin{flushright}
\end{flushright}
media campaign has a structured leadership and a core ideological center, it is still largely controlled by the collective messages and actions of its members.

Due to this unique aspect of ISIS’s propaganda machine, it is very difficult for law enforcement to track or combat this new type of ideological movement. The social media network of ISIS is so extensive, it can easily propagate its ideology through virtual media using the accounts of individual members. This decentralization allows ISIS members to easily spread their ideological followership around making it harder for authorities to identify and ban specific user accounts. Even influential ISIS Twitter accounts only have around 500 – 1,500 followers each, which makes it easy for them to repopulate on a new account should the original get banned. ¹⁰⁹ This new crowdsourced ideological movement is completely unique in the field of counter-terrorism. ¹¹⁰ However, this also means that ISIS may be subject to the actions and creations of its members, including anything that they could post on social media that would hurt the image of the organization.

Nevertheless, members have primarily adhered to the general narrative provided by ISIS in their online posts and social media activities. This narrative revolves around the Salafist Sunni interpretation of Islam that seeks to ban any innovation in society that was not present at the time of the Prophet Mohammad, as well as the rejection and destruction of all things and people that do not adhere to this philosophy. ¹¹¹ As opposed to Al-Qaeda, ISIS also presents its

narrative within the context of a tangible apocalypse, which will culminate with an imminent battlefield showdown between the peoples of the West and those of Islam.\(^{112}\) ISIS uses this narrative in conjunction with the current widespread unrest in the Middle East, portraying the US and its allies as evil apostates who are at war with Islam. The graphic images of violence such as beheadings and mass executions are used to provoke and intimidate the enemies of ISIS. They are also employed to capture the attention of potential recruits and reinforce the narrative that ISIS victory is inevitable. The terrorist group members also post pictures and media of a more jovial nature, often in the form of cat pictures.\(^{113}\) A more peaceful and humanitarian side of the narrative is included in ISIS propaganda as well, that promotes charity and other social welfare activity.\(^{114}\) These narratives may be appealing to the mind of young Western Muslims who all too often find themselves in a crisis of identity, living in a time of cultural division between the West and Islam.

Both case studies of Al-Qaeda and ISIS show that each organization engages in online recruitment and interaction through social media in a similar fashion to politicians or commercial entities. However, there are some key differences that should be highlighted. The online propaganda effort of ISIS is clearly more focused on utilizing social media than that of Al-Qaeda’s. The latter seems to be using social media with more frequency than it has historically, however its content and messages are still centered on a hierarchical, vertical system that

\(^{112}\) Prucha.


revolves around specific leaders and their directives.\textsuperscript{115} By contrast, ISIS utilizes its propaganda in a more interactive and communicative way with its followers primarily through social media. Personal videos and opinions of ISIS members and supporters are all included within the web-space of ISIS’s propaganda, and treated with a high degree of value. ISIS also produces sleek and highly edited propaganda videos that present a more collective and inclusive narrative in which all members are involved.\textsuperscript{116} Al-Qaeda presents its media as a form of directives to be followed, emanating from leaders within the group. ISIS offers its membership a collective narrative that is being experienced in real-time by everyone within the group, although its leadership does provide some guidance within this context. The primary reliance on social media as their vehicle for information dissemination further promotes this idea of collective experience within the membership of ISIS, as it is literally being propagated, talked about and experienced by the entirety of its membership in real-time.

ISIS in particular appears to follow the same themes of social media marketing as other mainstream organizations. One of the main themes of social media marketing is that it provides a real-time two-way conversation between businesses and their customers that is interactive in nature and makes the later feel included and in control, rather than having an advertisement forced upon them.\textsuperscript{117} The data above shows that ISIS adheres to this concept. As an example, one author describes the phenomenon of ISIS’s unprecedented twitter-sphere as a

“swarmcast.” 118 This massive network of interconnected twitter users are all interconnected to one another, and they receive messages not only from primary ISIS controlled accounts, but also one another. This allow for widespread, instantaneous and redundant communication and dissemination of information, which is nearly impossible to track or counter given its speed and range. 119 For example, the Shifa al-Sudur video of the captured Jordanian pilot Mohammad Kasasbeh was retweeted approximately 32,000 times in a mere 6 hours after its initial release by primarily ISIS accounts. 120 The effectiveness of this social media approach lies not only in the speed and range of its capability, but also in the fact that each time this video is tweeted, the ISIS member, supporter, or would-be recruit feels involved and actively engaged in the propaganda (or advertisement) process. They are not simply having directions given to them by some higher authority as is the case with Al-Qaeda, but are instead participating in the act of disseminating propaganda. This likely cements their support and belief in the organization as a whole, as they are actively invested and engaged with it. Such a phenomenon mimics the social media marketing strategies of major companies.

The risk of such social media marketing strategies is that the companies to which they belong inevitably give up some control over their content and direction. As such, companies encourage massive investment in large-scale social media campaigns and controlling organizations. 121 Our data shows that Both Al-Qaeda and ISIS have adopted this approach, although the latter has far outpaced the former in its investment in social media. The efforts of

118 Prucha.
119 Prucha
120 Prucha
121 Anand 7.
ISIS’s multiple propaganda centers such as Al-Hayat and Al-Furqan highlight the importance of propaganda efforts within the organization. Whenever ISIS captures a new town within its territory, a specialized propaganda team, usually consisting of at least six individuals, is sent to the location to film propaganda films not only for the local populace but also its worldwide audience. These propaganda efforts produce a large quantity of high quality videos and audio recordings that are then disseminated online via ISIS’s massive social media network led by its “media mujahideen.” Although Al-Qaeda has invested a massive amount of time, money and effort into its own propaganda operations, it is arguably lacking qualitatively in the digital media such as professionally edited videos. More importantly, Al-Qaeda lacks the same presence on social media as its counterpart, ISIS, which has an estimated 46,000 Twitter accounts that follow ISIS and help to disseminate its propaganda. This is perhaps a reflection of the lack of investment Al-Qaeda has put into its social media in comparison to ISIS.

Analysis of the data recorded indicates that our hypothesis is proven correct. Both case studies show that terrorist groups use social media in a similar format as major companies or even political leaders. It is also clear that ISIS utilizes social media far more than its counterpart,

---

123 Prucha.
124 Prucha.
Al-Qaeda. This raises several implications. Although ISIS is able to reach a wider base of individuals faster and engage them more thoroughly, it has a higher risk of losing control over the direction of its propaganda. However, it could also be argued that this lack of control is negated by the sheer magnitude of conversation on social media that all adheres to the same general narrative produced and controlled by ISIS. In other words, ISIS can ensure the legitimacy of its control by clouding any one individual’s opinion with voices of thousands of jihadists who all reaffirm the core narrative. This type of virtual peer-pressure ensures that everyone within the cyber sphere of ISIS social media stays on target with the narrative produced by the terrorist leaders and propaganda centers. Nevertheless, further research should be conducted over the possibility of dissent within the realm of ISIS virtual propaganda, given the client-oriented perspective of social media interaction.

Conclusion

Social media is a fairly new and quickly growing form of online interaction. Studies on the effects of these virtual relationships have given the commercial world a glimpse of how to utilize these tools and reap their rewards. Politicians have also begun to engage in social media interaction with their constituents. The effects and implications of this new phenomenon can also be seen within terrorist organizations’ use of social media. However, there remains a lack of information on the subject of terrorism and social media. This study has sought to contribute
to this lack of research by drawing parallels between the commercial world, and that of cyber jihadists within ISIS and Al-Qaeda. With ISIS serving as the flagship for the potentialities of terrorist use of social media, it is clear that this phenomenon will only grow in importance for our understanding of how such organizations grow, support and control their membership on a massive and virtual scale.
Chapter Three:
Theories of Homegrown and Organizational Terrorism in the Age of Global Virtual Communication

Introduction

For the last decade, studies on terrorist groups such as Al Qaeda have focused on a top down hierarchical organization that used interconnected cells to carry out large scale, mass casualty attacks on Western soil. As such, early academic work on terrorist use of the internet emphasized the operational components of the internet that allowed communication and logistical support between cells. Online propaganda and recruitment were also popular subjects, especially after the attacks by Nidal Hassan and the growing influence of Anwar al-Awlaki. However, “lone wolf,” or “homegrown terrorism has largely continued to be considered a separate category of terrorism. New terrorist groups such as ISIS are forcing scholars to rethink the differentiation between “homegrown” and organizational terrorism, especially in light of the growing importance of online connectivity throughout the globe. With this in mind, the thesis of this chapter will revolve around the following question: How does a terrorist organization’s online and social media capabilities affect the typologies of its recruits?

This question seeks to address the current gaps in the literature, to provide insight into the apparent conglomeration of homegrown and organizational terrorism, and to calculate the importance of online capability and strategy in a given terrorist group. ISIS will be used as a case study to determine these effects. It is an ideal candidate due to its current strain on global
security, as well as its unrivaled internet presence, which allows it to recruit both “homegrown” extremists and foreigners who will travel abroad to physically join ISIS. This is an important difference. There are several different categories of individuals that join ISIS who are often originally connected to that organization primarily through virtual interaction. We will distinguish between three types of ISIS recruits: satellite martyrs, foreign fighters, and wannabes. Satellite martyrs are individuals whose actual membership in the organization is ambiguous, but who have carried out (or attempted to carry out) acts of terrorism in the name of ISIS. Foreign fighters are those who travelled or attempted to travel to join ISIS in person, but had previously only been in contact with them through the internet. Finally, wannabes are a largely unknown grouping of individuals who engage in the virtual interaction with ISIS affiliated accounts or material and support their cause, but do not act illegally on their feelings for whatever the reason. The differences and definitions of these groups will be further expounded upon in the literature review section.

At the moment, ISIS seems to be facing a crossroads in its strategic use of online propaganda. While its social media efforts have increased both its recruitment of foreign fighters and its ability to inspire satellite martyrs, the barbaric and apocalyptic nature of some of their propaganda has led to international condemnation and a vigorous coalition counteroffensive. As ISIS continues to fight this tide of opposition, they will likely continue to utilize their social media machine to replenish their ranks on the battlefield and inspire homegrown attacks in an attempt to goad Western powers into attacking them and feeding into their narrative of The West vs. Islam. However, should they suffer significant territorial loses and subsequent de-legitimization, their appeal to foreign fighters may halt, and they
instead shift their focus to inspiring *satellite martyrs*. Information from case studies of ISIS recruits will give us a better understanding of the group’s capabilities and strategies. However, a review of the literature surrounding this subject will allow for a structured analysis.

**Literature Review**

The theoretical aspects of this study require a brief review of certain key concepts from previous chapters. Despite the various academic controversies surrounding the term, “terrorism” will be defined as it was in chapter one.\(^{127}\) The US Federal Code of Regulations defines terrorism as, “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.”\(^{128}\) With that in mind, both types of ISIS recruits will be considered terrorists. *Satellite martyrs* are obviously considered terrorists given their required criteria of having committed a documented terrorist attack. *Foreign fighters* who willing travel to Syria and Iraq to fight for ISIS also fall under the category of terrorism,


regardless of any lack of evidence as to their actual actions on the ground there, because they
have joined a terrorist organization.

A second term we must remember for this study is “radicalization.” In the words of
Peter Neumann, this is simple two-part process, although there are a variety of uncertainties
and variables that can go into a person’s decision-making process which academics may never
fully understand. Individuals experience radicalization by first becoming indoctrinated or
convinced of a set of beliefs that are contrary to main stream society and considered
“extreme,” and second (but not always) choosing to act violently against others.129 There are
several other processes of radicalization documented in chapter one that may also prove useful
in our analysis of ISIS online recruits.130

The final term for reconsideration is that of the “lone wolf,” or “homegrown” terrorist.
In chapter one, we accepted the term as defined by Spaaij and Weimann. Namely, that lone
wolves are “persons who (a) operate individually, (b) do not belong to an organized terrorist
group or network, and (c) whose modus operandi are conceived and directed by the individual
without any direct outside command or hierarchy.”131 While this term for a study of only “lone
wolf” terrorists, such a definition may suffice. However, for our study we must find a different
term of description for individuals that seem to meet one of two or these criteria

Source Complete.
Hill: University of North Carolina Press. 420-37; See also Olsson 17; Singer, M. 1995. Cults in our Midst: The Hidden
Menace in Our Everyday Lives. San Francisco: Jossey-Bass Publishers, 64-69; See also Olsson 16.
Research, 3(2): 75-90.
intermittently, but never all of them. For term (a), it is likely that our data will show ISIS recruits often operate individually or in smaller groups, but even if they are technically alone they may still have an unknown but significant amount of contact with the ISIS virtual community. This same factor of ambiguity clouds terms (b) and (c) for ISIS online recruits. Therefore, a new term is required that can conceptualize the relationship between organizational and lone wolf terrorism.

A dichotomy can be seen among ISIS recruits, which may provide insight into the mechanisms of online recruitment, as well as a framework for this study. ISIS members recruited online can be divided into three categories. “Homegrown” ISIS members are those who carry out isolated attacks in their home countries in the name of ISIS, but with little operational connection the group. However, the term homegrown is inaccurate as it suggests complete isolation from any active organization, which seems to be an obsolete concept in the face of powerful online propaganda strategies and interactive social media tools employed by ISIS. Therefore, we will refer to this group as satellite martyrs. This term has two defining criteria. First, satellite denotes that they are individuals who have no physical contact with actual ISIS members, but interact with them or their affiliates virtually, via online social networking or other internet media. Second, their eventual decision to carry out an attack in their home country in operational isolation signifies their deadly dedication to a cause that they are physically isolated from, but consider personally significant enough to merit an assault on others and their own martyrdom. The concept of martyrdom may seem academically controversial, but it is essential considering the religious and cultural background to which
many would be ISIS recruits are often attuned, as well as the tactical reality that most ISIS related satellite attacks ("homegrown" attacks) involve an individual fighting to the death.

The second group we will refer to as foreign fighters. These are individuals who come into contact with ISIS online and leave their home countries to successfully join ISIS on the ground in Syria and Iraq. To clarify, these individuals must successfully have made it to Syria and Iraq to join ISIS, and those who merely attempted the journey unsuccessfully will not be included in our analysis. The word “foreign” in foreign fighters highlights several key themes of this group. These individuals are foreign from the perspective of ISIS meaning they are not native to Iraq or Syria. However, language differences seem to be an easy hurdle for ISIS, as it has been documented that the group operates an extensive multi-lingual operation online.\textsuperscript{132} Furthermore, any differences between ISIS members and their “foreign” cohorts may often be overcome by shared ethnic, religious and cultural backgrounds between ISIS members and recruits.\textsuperscript{133} However, other scholars contend that it is uncertain whether such factors are important to ISIS recruits, as they are often quite ignorant of Islam despite their allegiance to the group.\textsuperscript{134} Nevertheless, these are important concepts to consider in our analysis of this category.

A third group, which we will refer to simply as wannabes, can be described as those who heavily support ISIS and would either join or launch an attack but do not because of state action, personal lack of commitment, or other unknown force of intervention. Despite their

\textsuperscript{132} Darrell D. Culbertson. ISIS/ISIL: The Islamic State Exposed, the Dangerous Truth You Need to Know! May 12, 2015. 83.
\textsuperscript{133} Culbertson, 81-82.
often lack of actual criminal activity and their satirical name, these *wannabes* should not be completely ignored as they often lawfully engage and interact with social media accounts and online material affiliated with ISIS. However, due to a lack of information on this last group, the *satellite martyrs* and *foreign fighters* will be the focus of this study on ISIS recruitment.

In order to understand the power and influence a terrorist organization can have over an individual through the internet is a key concept. There are several authors that discuss the importance of these virtual environments, and debate the efficiency of virtual and in-person radicalization. Neumann offers an early glimpse of how a virtual community can function. His studies on Al-Qaeda cells in Europe note that a terrorist community catalyzes an individual’s radicalization process by normalizing certain ideologies and behaviors for potential recruits.\(^{135}\) Although this description is in reference to actual physical interaction between group members and recruits, similarities seem to exist within the realm of online interaction as well.

Darrell Culbertson argues that these communities can exist virtually. He notes a variety of reasons behind an individual’s decision to join ISIS. High wages and access to war booty, a sense of belonging in a capable and morally superior community, and above all, a feeling of fulfillment and excitement in fighting for a cause that is depicted as righteous.\(^{136}\) This sense of community is heavily documented by media centers established in every ISIS controlled locale, and is broadcasted globally to potential recruits.\(^{137}\) Images and videos of infrastructure building, civil service and humanitarian aid are broadcasted to followers alongside the images of brutal

---


\(^{136}\) Culbertson 79-82

\(^{137}\) Culbertson 79
violence that dominate Western headlines. Furthermore, Culbertson argues that ISIS often implements Sharia law on the ground “piecemeal,” in order to placate the local populace and attract new recruits, which is reflected in ISIS online propaganda. Historical and geopolitical references are also implemented to explain and normalize the community’s behavior, such as the often referenced 1916 Sykes-Picot Agreement that led to the delineation of Arab state borders by European powers.

In accordance with Neumann’s theory on terrorist communities, this sense of a virtual community described by Culbertson is amplified by the projection of an actual community on the ground in ISIS controlled territory. This phenomenon of a terrorist organization being able to share massive volumes of media depicting life on the ground in a large area controlled by said organization is incredibly powerful. It is arguable that it provides a real sense of community to those who can only access it online and contributes to their radicalization process as if they were there with the group in person.

Another question within the literature of terrorist use of the internet and social media revolves around ISIS itself. There is a debate among scholars over the actual utility of ISIS’s social media capabilities. Max Abrahms explains that there are two schools of thought on the merits of its social media notoriety. The first, referred to by Abrahms as the ‘alarmists,’ believe that the social media efforts of ISIS are so unprecedented and effective at recruiting new members that authorities must focus on clamp down on these online activities. Abrahms

---

138 Culbertson 79-81.
139 Culbertson 82.
140 Culbertson 79.
supports the second group, which argues that although ISIS social media is having unprecedented effects on its recruitment, the brutal nature of their propaganda is actually working against itself by forging international cooperation against it and making it nearly impossible for the group to achieve its goals diplomatically, or even militarily. In fact, ISIS group size is lower in 2015 than it was when the group launched in 2011, which may be attributable to sheer battlefield attrition in the face of coalition forces. The answer to this question of the overall efficacy of ISIS’s online recruitment strategy in the context of their battlefield tactics may be outside the scope of this paper. However, their social media prowess demands further study of this phenomenon.

Theory and Hypothesis

The academic theories surrounding our study raise a host of questions for terrorism scholars. In order to determine the effects of ISIS’s social media strategies, a firm understanding of ISIS’s capabilities must be underscored. As noted in my second chapter and continues to be heavily documented, ISIS has a massive social media and online propaganda wing, which

---

142 Little.
generates and circulates its material globally on an unprecedented scale. It is possible that this level of virtual interaction creates an online community allowing for the radicalization processes described by Neumann and Culbertson.

It is hypothesized that ISIS’s tactic of both inspiring homegrown attacks and recruiting new membership are encouraged and enhanced by ISIS online recruitment and social media interaction. Earlier lone wolf cases examined by this paper could be divided into primary and secondary effects on the process of radicalization. However, the onset of social media combined with the ingenuity of ISIS internet capabilities could accelerate these effects simultaneously. Patterns of these satellite martyr attacks or foreign fighter recruits may provide a glimpse into what could become ISIS’s primary tool of terrorism should they continue or alter their strategies of online recruitment. Recent case studies on individuals radicalized over the internet with connections to ISIS will be evaluated in order to determine our hypothesis and better understand the new phenomenon of seemingly “homegrown” extremism exacerbated by online terrorist propaganda.

A second hypothesis will also be tested. It is predicted that ISIS has a specific social media strategy to target and recruit foreigners, particularly Westerners, as foreign fighters or satellite martyrs. Westerners offer a unique blend of strategic values for ISIS, for operational and logistical, as well as for recruitment and propaganda purposes. Finding evidence that supports this theory will help us to analyze ISIS’s social media strategies. It may also offer speculation as to why ISIS has chosen to focus on this particular pool of potential recruits.
If there is enough information from our data, we will also test a third hypothesis. It is hypothesized that *satellite martyrs* and *foreign fighters* are inspired to join ISIS by different types of ISIS propaganda material. Although both categories of recruits interact with ISIS virtual communities primarily through social media, it is possible that aspects of this propaganda effect these types of recruits differently. As an example, *satellite martyrs* may find themselves attracted to apocalyptic or violent styles of media, while *foreign fighters* are more inspired by themes of community belonging, religious morality or adventurism. While it will be difficult to accurately assess the motivations behind an individual’s decision to join a terrorist group, these motivations could provide insight on ISIS’s social media efforts.

**Methodology**

This study will attempt to prove three separate hypotheses using qualitative data derived from multiple case studies. Our first hypothesis will be proven correct in cases where *satellite martyrs* or *foreign fighters* interacted with ISIS primarily through virtual communities during their period of radicalization. The internet must remain the primary point of contact between potential recruits and the organization itself, in which their radicalization is enhanced or encouraged by the use of the internet, up until the point of their terrorist attack or physical membership in ISIS. Should an individual interact with an ISIS member in person outside of Iraq and Syria before their full indoctrination into the organization, they will prove our original
hypothesis incorrect. Contact between potential recruits in person will be included, but their exposure to actual physical interaction with other like-minded people should be noted in our analysis. Information such as the time spent in these virtual communities by recruits, as well as the type of interaction and media will also be examined in order to gain understanding of these relationships.

The second hypothesis will be proven correct if it is shown that ISIS recruitment strategies specifically target Westerners to become satellite martyrs or foreign fighters. Any evidence that strongly suggests or proves the deliberate targeting of Westerns for recruitment through social media and the internet will be analyzed for its support of this hypothesis. Understanding the intentions and strategic values of ISIS’s propaganda efforts will help authorities combat the organization and generally inform the academic discourse on this subject. In order to inform our discussion of social media recruitment strategies, we must also consider the content of ISIS propaganda and the virtual community in which it exists.

Finally, the last hypothesis will be proven correct if there are any aspects of ISIS’s social media and online radicalization efforts that are distinguishable between our two types of recruits, satellite martyrs and foreign fighters. This could include a particular category of media favored by ISIS such as religion, violence, geopolitics, community belonging or adventure. It could also include types of media such as twitter messages that are more interactive, or watching videos and looking at images. Although this information may prove illusive, they could offer important insight into the processes of radicalization in each type of recruit.
Our case studies will involve individuals foreign to Syria and Iraq who have been in contact with ISIS online prior to joining their organization. Cases will be examined between the years of 2011 and 2015, in order to give us a grasp of ISIS’s social media capabilities and strategies throughout the entirety of its existence. It is likely that the best qualitative information will come from cases originating in Western countries due to the availability of sources and the fascination with such subjects. According to recent estimates, there are now around 20,000 foreigners fighting in Iraq and Syria for ISIS, around 3,400 of which are from the West.\(^{143}\)

Comparing and contrasting the differences between *satellite martyrs* and *foreign fighters* may help us to understand the overall process of social media recruitment and radicalization.

**Data and Analysis**

First, cases of *foreign fighters* will be examined. Shannon Maureen Conley is the first of five case studies involving ISIS recruitment of foreigners. Conley is a 19 year old resident of Colorado who was arrested in April 2014 in the Denver airport attempting to board a plane to

---

Adana, Turkey to join ISIS. She was engaged by ISIS members online and eventually began virtual courtship with a 32 year old Tunisian member of ISIS fighting on the ground in Syria and Iraq. According to her parents, she would talk to her (unbeknownst to them) ISIS “suitor” on skype quite often. Five months before her attempted departure to Syria and Iraq, authorities interviewed her at least seven times in response to an anonymous tip and her online activities. While her sanity has certainly been questioned throughout her trial, she has repeatedly claims she did not know about the true brutality of ISIS and simply wanted to be a nurse for ISIS and “did not want to hurt anyone.” However, the same source also notes that she attempted to discuss violent jihad during religious visits with female imams inside prison. Her eagerness to help others as a nurse and marry a member of the organization suggest that she felt a strong sense of community through merely virtual interaction. It is also noteworthy to mention the differences between radicalization processes of men and women, as it would seem from this case as well as other cases, such as Collen LaRose, that females may be more motivated by personal relationships than males. The second case is that of Maxime Hauchard.

Maxime is a 22 year old male from a quiet town in Normandy, France. He converted to Islam at age 17 after watching youtube videos. Sometime after that he was contacted online

---

147 Martinez, Cabrera and Wesfeldt.
148 Martinez, Cabrera and Wesfeldt.
my ISIS recruiters, but never met with them in person and travelled alone to Syria and Iraq to join the group in 2013.\textsuperscript{150} Maxime appeared in an ISIS video released November 16, 2014 in which 14 Syrian soldiers and American aid worker Peter Kassig were beheaded.\textsuperscript{151} In his social media posts, Maxime posts pictures of himself holding weapons and has claimed that he supports the establishment of a proper Islamic caliphate and welcomes “martyrdom.”\textsuperscript{152} It is notable that, as far as we know, Maxime had absolutely no contact with ISIS members or anything regarding this type of extremist ideology in his life in rural France, except through his online experiences.\textsuperscript{153}

A third case study involves John Maguire, a 23 year old Canadian man who was recently charged by Canadian authorities with running a recruitment network on behalf of ISIS.\textsuperscript{154} Maguire left Canada for Syria and Iraq in December of 2012. Months before his disappearance, he was engaged with ISIS social media, and changed his name to Abu Anwar al-Canadi and Yahya Maguire on his social networking accounts.\textsuperscript{155} He would often post on the accounts of his friends criticizing them and demanding their repentance for living sinfully.\textsuperscript{156} In December of 2014, Maguire appeared in an ISIS video calling for other Canadians to either rise up and attack


\textsuperscript{151} “Enfant de la Patrie.” The Economist, November 18, 2014. \url{http://www.economist.com/blogs/charlemagne/2014/11/french-jihadi}

\textsuperscript{152} Penketh; Glum.

\textsuperscript{153} Penketh; Glum; “Enfant de la Patrie.”


\textsuperscript{155} Doug Hempstead and Keaton Robbins. “John Maguire was ‘lone wolf’ during final months in Canada.” Ottawa Sun, January 15, 2015. \url{http://www.ottawasun.com/2015/01/15/john-maguire-was-lone-wolf-during-final-months-in-canada}

\textsuperscript{156} Hempstead and Robbins.
their homeland or come and join ISIS abroad. Maguire offers a unique case in that his recent charges implicate two other men that were part of his recruitment efforts. According to authorities, Maguire was friends with a 25 year old man named Awso Peshdary before leaving for Syria. However, Peshdary remained in Canada and in contact with Maguire. The two began working together to recruit other Canadians to join ISIS, such as 23 year old Khadar Khalib, the third man implicated in the case who was recruited by Maguire and Peshdary and left for Syria and Iraq in March 2014. This recycling of successfully recruited foreign fighters shows that ISIS is motivated to recruit Westerners and is capable of doing it entirely through the internet.

The “Denver girls” case is another example of ISIS’s social media practices. Their story begins in April of 2014, when the three girls, ages 15, 15 and 17, posted on the mobile application AskFM the following question: “Would it be considered enough of a religious sacrifice to go to Syria simply to live and pray, but not to fight?” Multiple accounts claiming to be associated or representative of ISIS responded to girls query and began a process of indoctrination that lasted 6 months and included over 9,000 messages. They developed their closest relationship with two ISIS fighters on the ground in Syria and Iraq, and eventually agreed to come to Syria to join the group in person. At this time, an ISIS “facilitator” helped organize their trip and counseled them online for what to say at passport control in Turkey, which bus to take to the Syrian border and a phone number to call at the border to arrange a pick up. The

---

157 Hempstead and Robbins.
158 Campion-Smith.
girls were eventually stopped in Germany on their way to Syria and returned home.\footnote{Toby Temple-Raston.}

Considering their age, this case is remarkable in that these girls conducted this entire process through online social media completely undetected by their own friends or family. It also gives strong evidence to support the notion that ISIS specifically targets Western individuals.

The final case study of a \textit{foreign fighter} is that of a Canadian individual known to authorities through her Twitter handle, “L.A.,” and referred to popularly as “Toronto Jane.” This person was extremely active on her Twitter account in support of ISIS, and sometime after November 23, 2014, she made the trip to Syria and Iraq to officially join the group. Her reappearance in ISIS territory was discovered by the geolocation give off by her Twitter feed, which has subsequently documented her travelling throughout Syria and Iraq often near the frontlines of battle.\footnote{Jeff R. Weyers and Mubin Shaikh. “Toronto Jane: The First Woman to be Documented on the Front Lines with ISIS.” IBRABO, January 30, 2015. https://ibrabo.wordpress.com/2015/01/30/toronto-jane-the-first-woman-to-be-documented-on-the-front-lines-with-isis/} This would suggest that she may be directly helping in combat. However, this would be an oddity considering that ISIS women are forbidden from participating in the fighting and are instead relegated as brides.\footnote{Stewart Bell. “ISIS sympathizer’s road to jihad – from Canada to Syria to Iraq – tracked one Tweet at a time.” National Post, January 30, 2015. http://news.nationalpost.com/news/canada/isis-sympathizers-road-to-jihad-from-canada-to-syria-to-iraq-tracked-one-tweet-at-a-time} Interestingly, a report from 2015 by the Institute for Strategic Dialogue on ISIS female members notes that around 550 of the 3,000 Western ISIS members are women. On their case study of Canadian women, they conclude that Western women social media use shows their demographic prefers ideological propaganda that “portrays Muslims as victims of oppression, depicts such Western countries as sinful, and claims it is their religious duty to populate the ‘pure’ Islamic state.”\footnote{Stewart Bell.} As has been seen, almost all of
these cases involve individuals that undergo a radicalization process completely online, a process which is arguably accelerated by the virtual community of ISIS’s social media enterprise.

From the chosen case studies, the recruitment of foreign fighters seems to often take place between ISIS group members almost completely through social media and the internet throughout most of the process, and there also seems to be clear evidence of the deliberate targeting of Westerners. However, further case studies should be examined to determine the validity of this finding, as there is an inherent selection bias in the cases examined for this paper. This is primarily due to the large amount of information available on such cases of recruitment through social media and the internet on a case by case basis, as opposed to recruitment through other means.

A recent eyewitness account from an ISIS defector reveals that the terrorist group gives “special treatment” to Western recruits, particularly Europeans. The eyewitness goes on to explain that ISIS employs specific recruitment techniques once solid lines of communication are made with a potential Westerner. After a Westerner reaches out to ISIS via Twitter or some other form of social media, initial contact is then made between the group and the potential recruit via email. The recruit then undergoes a vetting process with ISIS recruiters through virtual communication channels such as voice over IP (VOIPs) programs or video chat programs like GoogleChat and Skype. Language translation software is used by recruiters if they do not speak the Western language of their target recruit. According to the source, this process is

---

extensive and carefully monitored by recruitment “emirs.” After passing enough online interviews, candidates are then directed to join ISIS through a variety of ways, usually by arranging travel to Turkey on their own and then crossing into Syria and Iraq with the help of local guides. Once they have been fully indoctrinated into the organization Westerners have shown they are capable of carrying out terrorist acts in the name of ISIS. One possible explanation for this online recruitment bias is the freedom of online movement provided by the Western world. The democratic values of Western countries and their strict adherence to freedom of speech laws extend into the virtual realm of the internet. In contrast, the countries in which many of these terrorist groups originate often suppress and monitor any online activity that is deemed a threat to their government.

After joining the ranks of ISIS through virtual interaction and eventually in person, Western recruits have shown that they are capable and willing to aid the terrorist organization and even carry out violent attacks. Some experts are uncertain or critical of the view that ISIS is purposefully recruiting Westerners. A recent report from the Rand Corporation noted that the unusually high numbers of Westerners travelling to fight in Syria and Iraq was more of a “spontaneous phenomenon” than any type of orchestrated event. The same source goes on to explain that the primary veins of foreigner recruitment are already established networks of foreign fighters on the ground in Syria and Iraq. These networks are all online and utilize social media to connect with one another as well as the communities and countries which they left.

behind.\textsuperscript{167} What this report fails to realize, is that these social media networks are acting on behalf of groups like ISIS to recruit and indoctrinate more Western fighters for their cause.

Once they are within these online jihadist circles the potential Western recruits can find various pathways to join ISIS. Westerners that make contact with ISIS affiliates via the internet can instantly find themselves surrounded by a virtual environment of like-minded Western jihadists via social media spheres. They can relate to and call upon the individuals over the internet for practical advice, ideological support, or simply social interaction. This virtual social network allows Western jihadists on the ground fighting for ISIS to indoctrinate and recruit new members.\textsuperscript{168} New recruits are encouraged to find their own way to Syria and Iraq to join in the fight, or simply launch homegrown attacks. Other evidence suggests that ISIS’s recruitment strategy is more structured and orchestrated by the terrorist organization itself rather than the twitter-spheres of its members. This is noted in chapter two as a potential side effect of ISIS’s social media capabilities.

Furthermore, ISIS has begun to call for homegrown attacks in Western countries. ISIS’s calls for homegrown attacks in Western countries has increased since the US-led coalition to destroy and degrade ISIS was formed in the summer of 2014. Since then, multiple small scale attacks such as the running over of two military personnel and the shooting of a third in Canada, as well as thwarted beheadings in Australia and numerous other attacks in Europe


have occurred. These seemingly homegrown attacks are attributed to what we have described as *satellite martyrs*.

We will look at several cases of these attacks in order to determine the effects of the internet on these individuals. According to a report from the US Department of Justice, officials are becoming increasingly concerned “about the possibility of homegrown extremists becoming radicalized by information available on the internet.” Evaluating these cases will help us to understand the validity of this concern and understand the effects of ISIS’s online recruitment.

The first case is that of Michael Zehaf-Bibeau, a 32 year old Canadian who shot and killed a Canadian soldier guarding a war memorial and then attempted to charge the Canadian parliament where he was shot and killed himself by security forces. He carried out his attack in October of 2014, a few weeks after Canadian Prime Minister Stephen Harper announced the country’s decision to join in the coalition to fight ISIS. Zehaf-Bibeau was born in Canada to a Libyan father and Canadian mother, both of whom were seemingly good and caring parents who raised their son in a loving environment. Around a decade before the attacks, Michael converted to Islam. Although some have suggested he was mentally unstable, a psychiatrist assigned to his criminal hearing in 2011 for robbery claimed that he was “unable to find any

---

features of signs of mental illness.” Notably, after his arrest in 2011, Zehaf-Bibeau asked to be imprisoned so that he could deal with his crack cocaine addiction and, in his own words, “spend time in jail as a sacrifice to pay for his mistakes in the past,” which he felt guilty about as a Muslim.

It is clear that his radicalization process involved the internet, as he was a follower of ISIS social media propaganda. He was also reported to be in contact via email with other like-minded jihadists in Canada, although it is not clear whether he was involved with these individuals in person. However, he was reportedly in contact with an Islamist fighter names Hasibullah Yusufzai through social media and frequently visited “Islamic extremist websites” and engaged in other online interactions with these jihadist circles. Notably, Michael attempted to leave Canada and travel to Syria or Libya, but was held up by passport restrictions. He traveled to Ottawa in early October, a few weeks before his attack, in an attempt to lift these travel restrictions.

A similar case is that of Martin Rouleau. On October 20, just two days before Zehaf-Bibeau’s fatal attacks, Martin Rouleau, a 25 year old Canadian, attacked two Canadian soldiers by running them over with his car in a parking lot before being chased down and finally killed in

---

a shoot-out with Canadian authorities. Martin Rouleau converted to Islam only a year before this attack, and was also involved with ISIS social media circles. After converting to Islam in 2013, Rouleau changed his Facebook name to Ahmed LeConverti (Ahmad the Converted) and began interacting with other Muslims as well as extremist circles via the internet. He reposted propaganda material such as videos and pictures that supported ISIS and its war against the West. Posts from months before the attack show that he was already undergoing radicalization, as he adamantly attacks the hypocrisy of “the disbelievers” and the punishments they deserve. Before his radicalization, Rouleau had a good relationship with his father who he lived with in St-Jean-sur-Richelieu, and did not have contact with any radical elements. Rouleau reportedly did not have any direct links to any other jihadist elements in person, which would suggest that his only contact with these circles was through the internet. Friends close to him noted that he “spent hours on the internet and devoured jihadist literature, adding that [he] dreamed of dying as a martyr.” As with the Zehaf-Bibeau, Rouleau had a his passport seized but attempted to travel to Syria to join ISIS in person before his attack.

Another case is that of Christopher Lee Cornell, a 20 year old man from Ohio, who was arrested in an FBI sting in January of 2015 for plotting to attack the US capitol building with

---

homemade explosive devices and automatic rifles. Cornell began making accounts on Twitter in the summer of 2014 under the alias Raheel Mahrus Ubaydah, in order to post and re-post videos, pictures and messages of ISIS propaganda. Cornell was completely unconnected to ISIS or jihadist elements in person. After his arrest, his parents claimed that he was in no way connected to these elements, and even accused the FBI sting operation of coercing their son into planning the attack. Whether or not this was the case, it is clear that Cornell became radicalized exclusively through his contact with jihadist circles via the internet.

The final case study is that of Alton Nolen, a 30 year old man from Oklahoma who was arrested for attacking two women, one of which he beheaded, that worked at the food processing plant where Nolen had worked and recently been suspended. The motivations for this attack are unclear and the FBI did not technically classify Nolan’s actions as a terrorist attack, although as a law enforcement agency the FBI would likely use whichever legal jargon can lead to a conviction. However, Nolan’s Facebook account shows he was very active and engaged with online jihadist propaganda. He posted several messages and images of violence, stating that images of beheadings and lashings were appropriate punishment for disbelievers under Islamic law. While the motivations surrounding his attack and the technical

---

classification as terrorism may be unclear, it is notable that Alton’s choice of beheading his former co-worker was seemingly inspired by his “affinity” for violence and his propagation of Jihadist material through online social media.186 Alton was raised as a non-denominational Christian and converted to Islam in prison during his incarceration for assault and battery of a police officer in 2011. Members of his local mosque noted that they were unaware of Alton’s extremist beliefs.187 This information suggests that Alton’s radicalization was largely effected by online propaganda rather than personal interaction with other like-minded individuals.

From the data, it is clear that our first and second hypotheses are proven correct. Interaction with online propaganda and ISIS jihadist circles seems to be a primary mechanism of radicalization in nearly all of our case studies. Furthermore, ISIS recruitment strategies appear to specifically target Westerners to travel abroad as foreign fighters or stay at home and launch attacks as satellite martyrs. Calls to participate in Jihad through either of these paths are prominent among ISIS social media propaganda and recruitment efforts. There does not seem to be enough concrete evidence to support our third hypothesis, as both foreign fighters and satellite martyrs engage in seemingly similar online activity before their decision to either join ISIS on the ground or launch an attack at home in the name of the organization.

Conclusion

The collected data gives us some insight into the overall recruitment strategies of ISIS and its online propaganda efforts. It is clear that ISIS propaganda and social media recruitment has targeted individuals, particularly Westerners, to either join the organization in person or simply conduct their own homegrown attacks. The dichotomy of what experts have traditionally considered “lone-wolf” or homegrown terrorism and organizational terrorism requires reconsideration in the face of this new threat. Further research on this topic is needed to understand and analyze the different ways in which ISIS and future terrorist organization are able to recruit and radicalize individuals almost entirely through the internet. More information is needed to analyze and understand the threat of online recruitment and radicalization by terrorist organizations. It is clear that this threat will continue to grow and pose unique challenges for counter-terrorism officials.
Bibliography

http://www.cnn.com/2014/10/22/world/canada-shooter/


[http://eprints.lse.ac.uk/46261/1/blogs.lse.ac.uk-The_trial_of_Anders_Breivik_shows_that_we_need_a_better_understanding_of_what_drives_rightwing_extrem.pdf](http://eprints.lse.ac.uk/46261/1/blogs.lse.ac.uk-The_trial_of_Anders_Breivik_shows_that_we_need_a_better_understanding_of_what_drives_rightwing_extrem.pdf)


Culbertson, Darrell D. “ISIS/ISIL: The Islamic State Exposed, the Dangerous Truth You Need to Know!” May 12, 2015


Kaplan, Andreas M. “If you love something, let it go mobile: Mobile marketing and mobile social media 4x4.” *Business Horizons*, vol. 55, no. 2, April 2013, p. 129.


Quan, Douglas. "ISIL a 'genuine risk' to Canada, expert warns; Revoking Canadian passports could cause extremists to move to act here." Ottawa Citizen, September 23, 2014. Lexis Nexis Academic.


Gregory Shuck was born in Wynnewood Pennsylvania on October 26, 1990. He graduated from Johns Hopkins University with a Bachelors in Political Science in May 2013, and continued his studies at Johns Hopkins for his Master’s degree in Global Security Studies from September 2013 to August 2015. He worked as a researcher at the University of Maryland’s National Consortium for the Study of Terrorism and Responses to Terrorism from June 2013 to July 2015 on various projects related to political violence and terrorism. Greg worked as a teaching assistant for a class on Responses to Terrorism at the University of Maryland in the Spring of 2015. Upon graduation from Johns Hopkins, he enlisted in the US Army in September of 2015.