5-2014

21st Century Radicalization: The Role of the Internet User and Nonuser in Terrorist Outcomes

David Wayne Woodring
University of Arkansas, Fayetteville

21st Century Radicalization: The Role of the Internet User and Nonuser in Terrorist Outcomes

21st Century Radicalization: The Role of the Internet User and Nonuser in Terrorist Outcomes

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts in Sociology

by

David Woodring
University of Arkansas
Bachelor of Arts in Criminal Justice, 2011

May 2014
University of Arkansas

This thesis is approved for recommendation to the Graduate Council.

_____
Dr. Kevin Fitzpatrick
Thesis Director

_____
Dr. Jeff Gruenewald
Committee Member

_____
Dr. Brent Smith
Committee Member

Abstract

This study examines differences between users and nonusers of information communication technologies (ICTs) within the pre-incident planning processes for domestic terrorist movements operating within the United States. In addition, this study is the first quantitative exploration of the prevalence, types, and purposes of ICT use within terrorist movements, specifically environmental, far-right, and Islamic extremist movements. Using "officially designated" federal terrorism investigations from the American Terrorism Study (ATS), we analyzed extracted evidence of ICT usage among individuals (n =331) engaged in the pre-incident planning processes as members of terrorist movements between 1995-2011. While we find significant differences in terrorist ICT use across terrorist movements, our findings suggest that demographics are not a strong predictor of usage. We find the highest prevalence of usage among Islamic movements. However, evidence of online radicalization or recruitment was found predominantly among environmental movements. We conclude with a discussion of these findings and their implications for counterterrorism policy.

Acknowledgements

I would like to thank my thesis advisor Dr. Kevin Fitzpatrick for his distinguished insight and instruction throughout the culmination of this thesis project. I would also like to express my gratitude to our department Chair Dr. Brent Smith, as well as the other faculty and staff involved in the research performed by the University of Arkansas' Terrorism Research Center for providing me with the technical expertise and tools to achieve greatness in my research.

Table of Contents

Introduction

The advent of information communication technologies (ICTs) at the end of the 20th century–specifically the convergence and integration of real-time telephone, computer, and wireless Internet networks–enabled Internet users to access, store, transmit, and manipulate vast amounts of information. With the creation of the Internet and social networking sites (SNSs), worldwide access to new information was disseminated around the world. With little distinction made between "online" and "offline," new technology has transformed our understanding of social space. As a result of this dynamic, the impact of ICT use on advancing the development of social movements harboring divergent ideologies, their access to one another, and their ability to distribute knowledge of their belief systems via the Internet has emerged as a burgeoning field of research **(**Friedland and Rogerson 2009; Garret 2006; Gillet 2003).

Of related importance has been the comprehensive analysis of ICT usage among grassroots, activist, and social movements, both old and new (Friedland and Rogerson 2009; Moussa 2011; Saeed, Rohde, and Wulf 2008; Shangapour, Hosseini, and Hashemnejad 2011). Appropriately, ICT usage among social movements such as terrorist movements has fallen under a similar scrutiny (Brachman 2006; Frieburger and Crane 2008; Jenkins 2010, 2011; OSCE 2008; Theohary and Rollins 2011; Thompson 2011; UNODC 2012; Weimann 2005, 2010, 2011, 2012).

The current analysis seeks to explore the prevalence, types, and purposes of ICT use within terrorist movements. With the understanding that not all terrorist movements are alike, the overarching question about how ICTs are used within the pre-incident planning process of domestic terrorist movements has brought the focus of this research to examine the ICT usage of

environmental, far-right, and Islamic extremist movements, the three most prominent terrorist movements operating in the United States over the past several decades.

The majority of research on ICT usage among the general population is divided between utopian and dystopian views of Internet use. Aside from the polarized examination and prediction of its effects, is the surprising absence of any comprehensive analysis of the characteristics of current ICT "users" and "nonusers" within unique subpopulations of grassroots, activist, or terrorist movements. Our analysis provides the first known quantitative examination of terrorist users and nonusers of the Internet within the pre-incident planning process of domestic terrorists in the United States. ICTs have proven to be powerful tools for social movements for both practical and social reasons (Coetzee 2008; Earl and Rholinger 2012; Gillet 2003; Shangapour, Hosseini, and Hashemnejad 2011; Youmans and York 2012). With a specific focus on terrorists–those who use violence or force against civilians or government to further a political or social cause–the types and purposes of ICT use have been explored in nascent literature, assessing both the documented and potential threats from these movements bearing violent political agendas (Brachman 2006; Frieburger and Crane 2008; Jenkins 2010, 2011; OSCE 2008; Theohary and Rollins 2011; Thompson 2011; UNODC 2012; Weimann 2005, 2010, 2011). The practical use of ICTs to spread information and network among these social groups has given social movements–those especially stigmatized and violent–a powerful voice that transcends geographical boundaries.

Users of ICTs among the general population are fundamentally different from nonusers in terms of their age, education, gender, marital, and socioeconomic status (SES) (Dijk and Hacker 2003; Hlebec et al. 2006; Kwon and Zweizig 2006; Roe and Broos 2005). SES has been one of the main correlates of ICT adoption and usage from the beginning of the information age

(Verdegem and Verhoest 2009). Therefore, it is reasonable to assume that the same demographic correlates of those who have both access to and use these technologies may correspond to or explain differences in ICT usage among terrorist movements. Extreme-left and environmental movements vary extensively from far-right movements in terms of their demographic composition. Extensive research shows that Internet users tend to be young (18-34), white, better-educated, full-time employed males, with considerable access to technology (Aerschot and Rodousakis 2008; Dholakia 2006; Robinson, Nuestadtl and Kestbbaum 2004; Roe and Broos 2005; Selwyn 2006; Selwyn, Gorard, and Furlong 2005; Verdegem and Verhoest 2009), all of which reflect the similar demographic composition of far-left and environmental movements. In contrast, nonusers tend to be under-skilled, less educated, concerned about privacy, have perceived costs and benefits for obtaining access, or simply may lack the financial resources to afford connection to the Internet (Aerschot and Rodousakis 2008; Selwyn 2005; Verdegem and Verhoest 2009). In the same way, these demographic and psychological correlates of nonusers are similar to members of far-right movements.

Furthermore, among the general population the Internet is primarily used as a means of communication and information/news dissemination (Cole 2008; Hlebec at al. 2006). The network neighbors of ICT users are geographically different and play less specialized, more functional roles in their lives (Hlebec et al. 2006). Accordingly, the geographic and organizational differences among terrorist movements may also drive differences in types and purposes of ICT use. The aforementioned literature suggests and supports the notion that the current research will likely expose varying prevalence rates of ICT use between terrorist movements for communication, information gathering/sharing, as well as differences in the demographic composition of users and nonusers of the Internet within the pre-incident planning

process. At the fundamental level, movements comprised of younger, better educated members may drive Internet usage within these movements; movements comprised of less-educated, older members such as the far-right may translate into less ICT usage due to lack of skills or access. Nonetheless, usage among terrorists may simply reflect the demographic kinds of differences among the general population with regard to skills and overall access.

The expanding reach of ICTs and SNSs has aided in the transformation of once hierarchical terrorist movements into decentralized social movements (Brachman 2006; Jenkins 2010, 2011; Weimann 2005, 2010, 2011, 2012). This aspect of social life merits not only an examination of how the Internet is being used by such movements, but how that use varies across different ideologies. Also important is an examination of the demographic characteristics of users and nonusers, within and between ideologies. Therefore, the present research intends to develop new analyses of existing terrorism data in order to gain a better understanding of who is using the Internet within domestic terrorist movements in the United States, how it is being used among these movements, and how specific uses vary between these movements. Accordingly, the analysis examines (1) the extant literature on the demographic correlates of users and nonusers of ICTs among the general population; (2) the emerging literature on types and purposes of ICT use among terrorist movements; and (3) the types and purposes of ICT use among the general population. This literature sets the foundation for the first quantitative analysis of terrorist users and nonusers of ICTs within the pre-incident planning process of domestic terrorist plots in the United States, as well as an exploration of the prevalence, types, and purposes of ICT use across environmental, far-right, and Islamic extremist movements. The findings will be compared to current literature on the correlates, types, purposes, and demographics of ICT users and nonusers among the general population, as well as the extant on

literature on both potential and documented terrorist uses of the Internet, to expand our current knowledge of both terrorist movements operating within the United States and the potential threat posed by such ICT usage.

Statement of the Problem

The nature of the potential and argued uses of ICTs among terrorists presents a significantly important social problem. Between the attacks of 9/11 and the end of 2009 a total of 46 cases of domestic radicalization and recruitment to jihadist terrorism were reported in the United States (Jenkins 2010). Over the past eleven years, prior research has documented over 170 individuals being indicted or identified in homegrown terrorist plots in the United States (Jenkins 2011). This research suggests that in many of these cases, radicalized, homegrown terrorists began their socialization through the Internet. According to aforesaid research, among Islamic extremist movements, many would-be jihadists appear to have begun their journey on the Internet in search of justification for grievances, affirmation of anger, solutions to personal problems, and even "the thrill of clandestine activity" in an epic struggle (Jenkins 2011). This, and other current research (Theohary and Rollins 2011; Thompson 2011; UNODC 2012; Weimann 2012), also indicates that by using social networking sites (SNSs) and interactive websites, the identity of individual and group grievances driving terrorist movements were easily found and reinforced through social networks of sympathizers as the Internet supported an open, non-confrontational environment where individuals were more apt to display their true feelings, emotions, and find an identity. Other literature illustrates that this process may be further exacerbated when Internet use is combined with face-to-face meetings such as in mosques, where individuals are indoctrinated and identity is also reinforced (Silber and Bhatt 2007). Nevertheless, quantitative research measuring the prevalence and role of such ICT use among

Islamic extremists or any other movement in relationship to the radicalization process of terrorists to violent extremism is nearly absent.

Apart from the radicalization of sympathizers, the preceding literature advocates that the Internet has become a primary medium of disseminating guidance and propaganda among terrorist movements. Research has found this type of practical use is notably prevalent among Islamic extremists. It is estimated today that Al-Qa'ida does 99 percent of its own work on the Internet (Jenkins 2010). Current research has established that terrorist movements, specifically those that are composed of Islamic extremists, are increasingly using ICTs for strategic operations to optimize their reach and inspire radicalization to violent extremism (Brachman 2006; Jenkins 2010, 2011; Theohary and Rollins 2011; Weimann 2005, 2010, 2011, 2012). What research has not established are prevalence rates of these types and purposes of Internet use among Islamic extremists, or among other ideologies such as environmental or far-right movements. Aside from the deficient measures of types and purposes of ICT use across these ideologies is the lack of quantitative research analyzing the demographic correlates of movements who use and do not use Internet within terrorist plots. The aforementioned literature has focused primarily on Al-Qa'ida and Islamic extremist movements, leaving the question open as to how other movements such as far-right or environmental movements may be using ICTs to further their cause.

As suggested earlier, the demographic composition of the aforementioned terrorist movements can vary broadly. Furthermore, the religious and ideological foundations of the far-right and Islamic extremist movements differ greatly from those driving environmental or "eco" terrorists. Accordingly, any assumption that ICT usage in relationship to violent extremism is limited to a particular philosophy or movements ideology may be potentially misleading given

earlier work suggesting important differences found in pre-incident terrorist activity among these three movements (Fitzpatrick, Smith, Roberts and Damphousse 2013). Admittedly, it remains challenging to provide comprehensive definitions of environmental, far-right, and Islamic extremist movements in the U.S., as they each have evolved over the last several decades in terms of their diverse motives, affiliated movements, and modus operandi. Nonetheless, it is important to offer broad descriptions of each ideological movement in order to contextualize anticipated findings of similarities and differences in ICT usage across movements. Thus, this study relies on Freilich et al. (2014) who undertook a comprehensive review of the literature in order to derive descriptions of each of the three ideological movements.

First, ***far-right extremists*** are described as:

> "…fiercely nationalistic, anti-global, suspicious of federal authority and reverent of individual liberties, especially their right to own guns and be free of taxes. They believe in conspiracy theories involving imminent threats to national sovereignty or personal liberty and beliefs that their personal or national 'way of life' is under attack. Sometimes such beliefs are vague, but for some the threat originates from specific racial or religious groups. They believe that they must be prepared to defend against this attack by participating in paramilitary training or survivalism" (Freilich et al., 2014, Appendix).

Second, Freilich et al. (2014, Appendix) have defined ***Islamic extremists*** as those who:

> "…believe that only acceptance of the Islam promotes human dignity. Islamic extremists reject the traditional Muslim respect for "People of the Book," (i.e., Christians and Jews). They believe that "Jihad" (i.e., to struggle in the God's path like the Prophet Muhammad), is a defining belief in Islam and includes the "lesser Jihad" that endorses violence against "corrupt" others. Islamic extremists believe that their faith is oppressed in nominally Muslim Middle-Eastern/Asian corrupt governments and in nations (e.g., Russia/Chechnya) that occupy Islamic populations. The U.S. is seen as supporting the humiliation of Islam, and exploiting the region's resources. They believe that America's hedonistic culture (e.g., gay-rights, feminism, etc.) negatively affects Muslim values. Islamic extremists believe that the American people are responsible for their government's actions and that there is a religious obligation to combat this assault. They believe that Islamic law- Sharia- provides the blueprint for a modern Muslim society and should be forcibly implemented."

Third, ***environmental extremists***:

> "…endorse biodiversity/biocentric equality (i.e., that humans' have no legitimate claim to dominate earth). They believe that the earth and animals are in imminent danger and that the government and corporations are responsible for this danger that will ultimately result in the environment's destruction. These extremists believe that the "system" is incapable of taking actions to protect the environment and biological diversity. Thus, there is a need to defend the environment and animals" (Freilich et al., 2014, Appendix).

Due to the lack of available terrorism data, comprehensive quantitative analyses of types, purposes, and the frequency of ICT and social media usage within pre-incident planning and/or violent extremism has been absent in the literature (Institute for Strategic Dialogue 2011; Silke 2008). Quantitative data on terrorist use of the Internet in relationship to radicalization is deficient (Institute for Strategic Dialogue 2011; Meehan, McCants, Weisburd, Jenkins, and Kohlmann 2011; Myrick, Thompson, Gannon, and Nuemann 2011; Silke 2008). Still, considerable qualitative and descriptive work has explored both documented and potential types and purposes of ICT and social media usage among terrorist movements, underscoring the importance of establishing prevalence rates among these other movements to provide important insight into this growing body of literature (Brachman 2006; Frieburger and Crane 2008; Jenkins 2010, 2011; OSCE 2008; Silber and Bhatt 2007; Theohary and Rollins 2011; Thompson 2011; UNODC 2012; Weimann 2005, 2010, 2011, 2012).

In addition to understanding prevalence rates among movements, also absent from current literature are quantitative analyses of how the Internet is being used and how this use may vary between movements. The Internet offers all the practical utility for research, propaganda, communication, information sharing, claiming responsibility for attacks, training, target selection, creation of websites, cyber-attacks, publicity, radicalization, threats, and recruitment (OSCE 2008; Theohary and Rollins 2011;Thompson 2011; UNODC 2012; Weimann 2004, 2005, 2010, 2011, 2012). However, the majority of the work that examines the process of

radicalization to violent extremism in relationship to ICT use has been either qualitative or anecdotal and generally lacking systematic comparisons or control group analysis (Myrick et al. 2011; Silke 2008).

To explain the differences in rates and uses within and between movements, the current research looks to demographic factors for a more complete understanding of what might explain any variation in use. Quantitative analyses have been performed on a variety of predictors of Internet use among the general population (Brandtzaeg 2012; Czaja and Lee 2007; Dholakia, 2006; Rodousakis 2008; Ryan and Xenos 2011; Selwyn, Gorard, and Furlong 2005). However, any connection to terrorist use, or how these might be related to the processes of pre-incident planning or radicalization to violent extremism, is minimal. Aside from the practical use by such movements, there may be a deeper connection to understanding how and why these movements and individuals within these movements use the Internet in general, or more specifically as a tool for radicalization. Likewise, the three movements being examined (environmental, far-right, and Islamic extremist) have very different motives and philosophies driving their movements; the way they use the Internet and social media might vary, particularly given the specific user characteristics and grievances that they often express. Thus, the current research seeks to create a demographic typology of users and nonusers of the Internet within domestic terrorist plots while comparing those findings to those of current studies examining demographic differences among the general U.S. population.

Study Significance

Over the past several decades, the dynamics of terrorist organizations and movements have evolved into a multidimensional threat (Gaibulloev, Sandler, and Santifort 2012; SPLC 2009). Once understood as a group phenomenon, the leadership and organizational structure of

terrorist movements today differ from the once hierarchical, state-sponsored initiatives (Ressler 2006). Inherently, many of these characteristic changes are reflected in both the planning and outcomes of domestic terrorist plots in the United States. Moving from the pyramidal and "hub-and-spoke" cell structures found in the 70s and 80s, the concept of "leaderless resistance" was facilitated and popularized by groups such as the far-right movements in the late 80s and throughout the 90s. The fundamental concepts underlying the leaderless resistance movement leveraged on the advantages of autonomous networks or cells of individuals sharing the same ideology, having no centralized authority or chain-of-command (Leader and Probst 2003). While the perpetration of terror attacks by individuals is no new phenomenon, there has been a growing prevalence of terrorist incidents in the United States committed by individuals (Weimann 2012). These acts have occurred under instruction from others and in rare cases have been the result of self-radicalization.

During the late 80s and early 90s, far-right leaders such as Louis Beam and David Lane motivated a resurgence of radical right activity by advocating the leaderless resistance as an effective strategy for avoiding detection, infiltration, and prosecution by government agencies (Joosse 2007). By the mid to late 90s, the environmental terrorist movements such as the Animal Liberation Front (ALF) and Earth Liberation Front (ELF) were also benefiting from a leaderless resistance operational structure (Leader and Probst 2003). Together, the ALF/ELF coalition caused damages in excess of $40 million between 1996 and 2002. Combined with the minimal preparation time required for arson, sabotage, and vandalism as the preferred methods of attack, the leaderless resistance model allowed ELF to become the most notorious and destructive "ecoterrorism" movement in the United States by the early 2000s. However, while a multi-

agency investigation was dismantling the ELF Family's infrastructure and arresting its members, the United States experienced an even more destructive terror attack.

As the threats to homeland security and effects of domestic terrorism in the U.S. were already changing, the landscape of domestic terrorism was dramatically altered even further after the attacks of September 11, 2001, as movements with similar "bottom-up" strategies surfaced. Although Al-Qa'ida's infrastructure was nearly destroyed by U.S. military efforts after the attack, an Islamic-inspired leaderless resistance evolved and added to an already existing multidimensional terrorist threat (Jenkins 2010, 2011; Weimann 2005, 2010, 2011, 2012; Silber and Bhatt 2007). Although there are a number of Islamic extremist movements, Al-Qa'ida has been the focus of much terrorism research. Al-Qa'ida conducts operations in the Arabian Peninsula (AQAP), Iraq (AQI), and Maghreb (AQIM), among many other regions of the world. Joining forces with other Islamic movements, threats have emerged internationally and domestically for the U.S. From allies such as al-Shabab in Somalia, to the Pakistani Taliban who trained the 2010 Time Square bomber and U.S. citizen Faisal Shahzad, the diversification of domestic terrorist threats is still growing (Bergen, Hoffman, and Tiedemann 2011; U.S Executive Office of the President 2011, 2011).

The Islamic leaderless movements, as well as other terrorist movements, have manifested themselves in many different forms. While there is no absolute consensus on how to define the different forms of "homegrown" radicalization to violent extremism in America, the following incidents illustrate various ways in which domestic attacks have been organized and carried out in the U.S. For example, Umar Farouk Abdulmutallab, with the help of Al-Qa'ida in the Arabian Peninsula (AQAP), attempted an unsuccessful "solo" attack against flight NWA 253 on Christmas Day, 2009. The 2009 Little Rock recruiting office shooting, perpetrated by

Abdulhakim Mujahid Muhamaad, was another example of a solo-attack. It should be noted that both of these incidents involved prior contact with terrorist operatives. However, the Fort Hood shooting in 2009, carried out by Nidal Hassan, required no previous contact with operatives at all. This type of "lone wolf" attack committed by Hassan is an example of the homegrown radicalization to violent extremism occurring in America that is raising concern. While the Islamic threat has occupied much of the research and public concern, such concern may have overshadowed terrorist movements such as those composed of environmental and far-right members that continue to thrive in the U.S. (Leader and Probst 2003; SPLC 2009). Likewise, while ICTs have emerged as playing a key role in the process of domestic radicalization here in the United States, the trends in literature have also focused almost solely on Al-Qa'ida and Islamic-inspired movements. However, in an IT-driven era, ICTs are viable tools readily accessible for strategic use among all terrorist movements meriting the necessity of this analysis.

From 2006 to 2012, ICT proliferation grew from 73 percent to 78 percent in the United States (Czaja and Lee 2007; Internet World Stats 2013). In addition, social networking site (SNS) usage from 2008 to 2010 grew from 35 percent to 61 percent among the general adult population (Pew Internet 2010). Currently, the number of SNS users in the world numbers over 1.2 billion with Americans spending 22% of their time on the Internet on these sites (Sheldon 2012). As ICT use expands, social scientists have a unique opportunity to examine differences between users and nonusers within social movements. Along with these powerful social tools comes the ability to amplify many aspects of social life. Not only does social life shape the Internet, but also the Internet is altering society in extraordinary ways, for better or worse. ICTs are proving to be valuable tools for of improving political engagement, increasing the efficiency of communication, and increasing productivity (Chinn and Fairlie 2007; Norris 2001;

Steinmuller 2001). The Internet is not merely a technology; rather, it possesses different meanings, purposes, and uses facilitated by differences among individuals and groups (Sewlyn 2006).

Accordingly, culture plays an important role in the way both individuals and groups adopt technology (Anandarajan, Igbaria, and Anakwe 2002; Ein-Dor, Segev, and Orgad 1993; Kumar, Ganesh and Echambadi 1998; Rogers and Shoemaker 1971; Schepers and Wetzels 2007; Straub, Keil, and Brenner 1997; Takada and Jain 1991), specifically the Internet (Pavlou and Chai 2002). Just as culture plays an important role in the adoption of ICTs in certain countries, the same applies to social movements, such as the aforementioned terrorist movements, and therefore adoption of ICT usage may differ depending on the users' origins, ideologies, and philosophies. As the social world changes with the technological innovations around ICTs, it has become important to understand how these technologies may be influencing terrorist outcomes.

Finally, previous research on tools used by terrorists in the incident planning process has focused primarily on explosives (Nambayah and Quickenden 2004; Ronald 2003; Slater and Trunkey 1997; Smith, Damphousse, and Roberts 2006); however, few studies have empirically evaluated the Internet as a terrorist tool. Furthermore, although "homegrown" terrorist activity may not be as prevalent as group oriented activity, theorists continue to argue that attacks by movements and by lone individuals will be more complex and sophisticated with the use of ICTs (Nesser 2012). In an era of IT-driven globalization, the expansion and use of these tools around the world to effectively further the cause of violent extremists has made terrorism an important social problem. ICTs have not only contributed to the globalization of information, they have also contributed to the globalization of terrorism (Hutchinson 2006). The targeting of vulnerable communities/individuals is a growing problem. Radicalization and counter-radicalization

initiatives at the Federal, state, and local levels are needed to prevent the recruitment and radicalization of individuals to violence (U.S. Executive Office of the President 2011, 2011). There is a specific need for research and initiatives by nongovernmental organizations (Myrick et al. 2011). Accordingly, recent academic and policy research has both been developed and been solicited in order to counter radicalization to violent extremism in the United States (U.S. Executive Office of the President 2011, 2011). A key aspect of such policymaking and research is aimed at understanding the vulnerable communities and/or individuals who may either use the Internet as a tool to recruit or be recruited. There is an evident and growing need to understand how communities and/or individuals use the Internet. Along with assessing these community-level threats comes the necessity to educate the public. Ideologically, the movements under examination are very different as the aforementioned literature purports, and the Internet is an important social extension of social movements and must be thoroughly understood.

Review of Literature

The current research requires a focus on three primary bodies of literature that help delineate the complex processes of ICT usage among and between various terrorist movements: 1) correlates or "predictors" of ICT users and nonusers among the general population, 2) terrorist use of the Internet from both a practical and psychological perspective, and 3) types and purposes of ICT use among the general population.

Characteristics of ICT Use among the General Population

To increase understanding of those who use ICTs within the pre-incident planning process of domestic terrorist plots first requires a general understanding of ICT usage among the general population. Within this context, this review begins with an examination of the impact of

ICT and SNS use on societies and individuals to understand the fundamental conditions from which the majority of ICT savvy individuals and societies operate. After this, predictors, motives, and social needs that distinguish Internet users from nonusers are reviewed. Again, any relationship between correlates of Internet use among the general population and those among terrorist movements have not been explored. Finally, the current qualitative literature that has inspired the quantitative analysis and variable selection for this study is reviewed with a specific focus on how this literature can explain individual and group variations in prevalence, type, and purpose of Internet use.

General ICT Use and Impact

ICT and SNS proliferation in the United States continues to increase significantly each year (Czaja and Lee 2007; Internet World Stats 2013; Pew Internet 2010). Sociological research on their use, nonuse, and impact on society is expanding as quickly as these technologies pervade social life. While much of the prior research focuses on the positive and negative effects of Internet use upon individuals, there is a growing body of literature on how ICTs, such as social networking sites (SNSs), have become powerful social tools and human culture and society (Hlebec, Manfreda, and Vehovar 2006). Accordingly, these technologies possess different meanings, purposes, and uses facilitated by differences between individuals and groups (Sewlyn 2006).The unique placeless environment within cyberspace, combined with asynchronous forms of communication fostered by ICTs, makes them powerful tools with the ability to amplify many aspects of social life. Not only has society shaped the Internet and its uses, the Internet continues to transform social life in extraordinary ways–some for better and some for worse–justifying much of the concern around online radicalization and self-radicalization.

Interest in and promotion of ICT use around the world has been spawned by the prospect of harnessing the power of these tools to improve cultural, social, and human capital (Chinn and Fairlie 2007; Norris 2001; Steinmuller 2001). Early research on ICT use facilitated rather dystopian views, correlating Internet use to loneliness, depression, lower self-esteem, introversion, as well as displacement of social networks and activities (Kraut et al. 1998; Korkeila, Kaarlas, Jaaskelainen, Vahlberg, and Taiminen 2010). Nonetheless, the impact of ICT use has changed as quickly as the developments of ICT itself. Current research refutes many of those early claims, showing ICT use has limited impact on psychological well-being and can actually be viewed as an extension of social relationships, increasing interpersonal communication (Chen and Persson 2002; Hlebec et al. 2010). ICTs increase international and geographic knowledge, awareness of world problems, have benefited disadvantaged minorities, allowing them to change their social standing, transforming users both psychologically and emotionally (Beaudon 2008). Latinos and African Americans are among the fastest growing population of users (Cole 2004). As ICTs have taken the place of traditional media, most users access the Internet for news and information. This trend has remained the same over the past decade, while an increase in Internet use for social networking has increased (Cole 2004; Hlebec et al. 2010; Korkeila et al. 2010). Online communication serves purposes different from those engaged in offline communications. The Internet is used more for functional purposes, which tend to be more task-oriented and impersonal. Although intensive Internet use is linked to spending less time on some activities such as sleep and work (Korkeila et al. 2010), it appears that ICT use does not displace important social activities but augments communication and social networking (Robinson and Martin 2009). Overall, ICT users tend to have healthy lives, sleep a little less, and participate in a little more physical activity.

Conversely, there are contexts in which ICT usage has not yet penetrated into the lives of individuals and communities. Therefore, understanding the background characteristics of the differences between those who use ICTs and those who do not among the general population is paramount to extrapolating why terrorist individuals and movements may or may not use ICTs in the incident planning process. Given the Internet's ability to enhance many aspects of social life, it becomes apparent that users are characteristically different from nonusers. The next section assesses the specific differences between users and nonusers of ICTs within the general population to further infer the likely parallels between this population and the population of terrorists selected for this analysis.

ICT Users and Nonusers

ICT users are intrinsically and fundamentally different from nonusers in terms of their age, education, gender, marital status, and socioeconomic status, which all have an impact on the probability of using the Internet, making demographics an important and often strong predictor (Dijk and Hacker 2003; Hlebec et al. 2006; Kwon and Zweizig 2006; Roe and Broos 2005). SES has been one of the main correlates of ICT adoption and usage from the beginning of the information age (Verdegem and Verhoest 2009). Again, comprehensive research shows that Internet users tend to be young (18-34), white, better-educated, full-time employed males, with considerable access to technology (Aerschot and Rodousakis 2008; Dholakia 2006; Robinson, Nuestadtl and Kestbbaum 2004; Roe and Broos 2005; Selwyn 2006; Selwyn, Gorard, and Furlong 2005; Verdegem and Verhoest 2009). The social networks of ICT users are different than those of nonusers, facilitating qualitatively different interpersonal roles for users (Hlebec et al. 2006). Men, persons 30 years of age or younger, use the Internet more for chatting and

discussion and have shown a higher tendency to be addicted to the Internet (Korkeila et al.). However, the gender gap in ICT usage has narrowed over the last several years (Selwyn 2006).

In contrast, nonusers tend to be under-skilled, less educated, concerned about privacy, have perceived costs and benefits for obtaining access, or simply may lack the financial resources to afford connection to the Internet (Aerschot and Rodousakis 2008; Selwyn 2005; Verdegem and Verhoest 2009). Elderly people have the lowest adoption rate and level of use of information communication technologies among all age categories (Flanagan and Metzger 2001). Social structure and the personal circumstances of individuals seem to drive use overall (Selwyn et al. 2005). At the macro-level, not only income, but regulatory effectiveness, telecommunications infrastructure, and human capital drive use of the Internet (Chinn and Fairlie 2007; Dasgupta 2001; Wallsten 2005). However, overall, income seems to drive Internet use among industrialized nations (Chinn and Fairlie 2007; OECD 2001; US Department of Commerce 2002; Quibria et al. 2003). Given the considerable research on what drives ICT use, a significant body of literature is also growing pertaining to users and nonusers of social media.

SNS Users and Nonusers

Social networking sites (SNSs) allow users to articulate and control a perception of their private lives to the public (Haythornthwaite 2005). Many introverted and lonely people with low levels of self-esteem, who seek to build these online social networks, are dissatisfied with traditional face-to-face interactions (Ong, Chang, and Wang 2011; Sheldon 2012); these sites substitute for traditional face-to-face interaction. These sites also offer unique networking opportunities to gain social approval and express opinions among its users (Gangadharbatla 2008). The SNS with the most profound effect to date is Facebook, a "Six-Degree-Separation" social networking site (6SNS) that allows users to maintain weak, but more effective ties in

terms of enhancing social activities and information sharing (Shu and Chuang 2011). Weak ties have actually been shown to be more effective for instrumental purposes such as finding employment or obtaining other important information (Hlebec et al. 2010; Shu and Chuang 2011). Similar to the research on traditional ICT use, current research finds no relationship between time spent using SNSs and size of social networks, or differences between network size or emotional closeness to others between users and nonusers (Pollet, Roberts, and Dunbar 2011). However, one recent study did find that male SNS users are lonelier than female users and nonusers, but overall users showed a significant increase in number of acquaintances and social capital (Brandtzaeg 2012). Other research has found interesting correlations between SNS use self-promoting and superficial behaviors, such as posting photos and writing status updates (Buffardi and Campbell 2008, Mehdizadeh 2010). In addition, research in the same vein is finding that users of 6SNSs such as Facebook have higher levels of total narcissism, exhibitionism, and leadership then nonusers (Ryan and Xenos 2011). Unlike general Internet use, SNSs have been used more by women than men (Sheldon 2012). Tufekci (2008) found that the best predictors of not using SNSs were male; concerns about personal security, less need to engage in social browsing, and instrumental versus expressive preferences for Internet use. Age is also a predictor with the most active users of SNSs being millennials (18-34) followed by teens (12-17). Sheldon (2012) found that age was the best predictor of nonuse; this work also found that the average age of nonusers of SNSs was 35.

As illustrated, interest in, and promotion of ICT use around the world has spawned considerable research and quantitative analyses on a variety of predictors of Internet use among the general population. However, any connection to terrorist use of the Internet, or how these correlates might drive the processes of radicalization to violent extremism is minimal. Again,

there may be a deeper connection to understanding how and why both groups and individuals, terroristic, or civilian, use the Internet in general, or as a tool, or are radicalized by those who do so. Likewise, the three movements being examined (environmental, far-right, and Islamic extremist) may have very different motives and philosophies driving their movements; the way they use the Internet and social media may also differ given the specific user characteristics found and grievances expressed. Therefore, the next section moves from use and nonuse among the general population to both the documented and potential terroristic uses of the Internet. After establishing the correlates of use and nonuse among these three movements, the goal is to extrapolate why and how terrorists are using the Internet and what factors might drive differences in ICT usage across terrorist movements.

Terrorist Use of the Internet: Prevalence and Type

To expound on the work described in the previous section and increase the understanding of ICT usage among terrorist movements, the current research additionally requires focus on three primary literatures that help delineate the complex processes of ICT usage among and between various terrorist movements: 1) prevalence of Internet use among terrorist movements, 2) terrorist use of the Internet from a practical perspective, and 3) terrorist use of the Internet from a psychological perspective. Moving from literature on the individual demographic characteristics of users and nonusers, the goal is to examine the potential and documented terrorist uses of ICTs, drawing inferences from factors that may drive differences in use across movements.

Prevalence of Use

As mentioned above, previous research has both documented and argued that ICT use, with a specific focus on Islamic extremist movements such as Al-Qa'ida, has become an

essential terrorist tool for disseminating guidance and propaganda (Jenkins 2010). While this research has primarily focused on the locus of Internet use within Islamic extremist radicalization, it has failed to examine the same process occurring in other domestic terrorist incidents or plots. Although terrorists can be categorized as radicals committing violent acts with the goal of achieving a broader social or political change, their ideologies, methods of recruitment, and targets have been very different (LaFree and Bersani 2012; Smith and Morgan 1994). It is likely that these differences are reflected in their ICT usage as well. Moreover, with the recent return and diversification of far-right extremism (SPLC 2009), data on Internet usage in the pre-incident planning and radicalization processes among movements other than Islamic-inspired extremists is needed to assess threat levels among these movements while at the same time creating proactive counterterrorism strategies proportionately.

Practical Use

For many terrorists, the Internet offers the practical utility of research, propaganda, communication, information sharing, claiming responsibility for attacks, training, target selection, creation of websites, cyber-attacks, publicity, radicalization, threats, and recruitment (OSCE 2008; Theohary and Rollins 2011;Thompson 2011; UNODC 2012; Weimann 2005, 2010, 2011). The Internet provides an efficient use of information gathering and sharing. From accessing the coordinates of a target's location on Google Maps to the distribution of bomb-making instruction manuals, the efficiency of the planning and communication process of terrorists has become increasingly accurate, and ICTs have facilitated in changing the rules of the game. Additionally, current research has suggested that new social media is being readily used to disseminate propaganda, reach and train group members, and aid in terrorists' ability to radicalize individuals (Brachman 2006; Freiburger and Crane 2008; Jenkins 2010, 2011;

Theohary and Rollins 2011; Thompson 2011; UNODC 2012; Weimann 2005, 2010, 2011); the Internet and new media offer an expanding list of tools for terroristic use.

In addition to practical purposes of general Internet usage, new social media offers radicals a way to promote the agenda of their movement and its often-complicated ideology. In the case of homegrown violent extremists, terrorism appears to be as much an expression of an identity as it is an ideology, and the Internet contains an ample supply of imagery, music, and text from which the aspiring terrorist can assemble a developing identity (Meehan, McCants, Weisburd, Jenkins, and Kohlmann 2011). Within social networking sites (SNSs), it is now easier to communicate with others and assimilate into almost any social network than it ever was before. Currently, researchers have found that 90 percent of terrorist activities on the Internet take place using SNSs, including independent bulletin boards, Paltalk, Yahoo or eGroups (Weimann 2010). The dramatic growth in the number of jihadist websites and chat rooms, especially the significant increase in English-language sites in this category from a handful to hundreds, has made the narrative and message of violent jihad more accessible and compelling to those who cannot read or speak Arabic (Jenkins 2010).

With the increased popularity of SNSs such as Facebook, Twitter, and YouTube over the past decade, a new social network environment and potential threat for terrorist activity has emerged. This environment is clearly conducive to expanding the reach of social networks, but it holds potential to amplify violent extremism (Klausen, Barbieri, Reichlin-Melnick, and Zelin 2012). These three SNSs in particular can offer terrorists the advantage of real-time updates, access to personal information, information sharing, and training capabilities worldwide. For example, YouTube is not merely a video-hosting site, but also a formidable social networking forum that can effectively promote violent acts, broadcast threats, and announce as well as direct

events and demonstrations (Meehan et al. 2011). Again, these potential uses justify potential concern and threats of such use.

With over 1.2 billion active users on Facebook, this SNS has been shown to pose a formidable threat to national security and is hard to regulate due to the First Amendment protection of US-based ISPs (Weimann 2010). Terrorists have been documented using Facebook to establish friendships through the "narrow casting" strategy by using the name, accompanying default image, and information on a group message board that were all tailored to fit the profile of particular social groups (Weimann 2001; 2010). Facebook also contains personal information about individuals, which poses security threats to military operations. In addition to compromising soldiers' accounts, Twitter with its now 500 million plus users poses a similar, but in some ways, unique threat. For example, Twitter enables terrorists to send and receive near real-time updates on the logistics of troops' movements in order to conduct more successful ambushes (Weimann 2011). Perhaps a more realistic threat is Twitter's political environment and asynchronous communication environment, which also has the potential to foster radical narrative.

All SNSs considered, the Internet holds various powerful methods of communicating and expanding social networks. Considering the far-reaching practicality of SNSs along with literature on Al-Qa'ida's usage of SNSs, it is likely that while Al-Qa'ida and associated Islamic extremist movements may be the most prevalent ICT users for communication and social networking, environmental and far-right movements may have adopted or developed similar ICT use strategies unique to the goals of their ideology. Research shows that movements are becoming aware of this capacity and even modeling their SNSs with similar design and logos to market their brand (Weimann 2011). For example, terrorists have been documented branding

their own versions of video sharing sites modeled after YouTube. Creating their own websites and linking them with a domain name allows the posting and cross-posting of radical content with less chance of detection or removal. Therefore, it is crucial to examine all types of SNS and Internet usage may occur in the pre-incident planning process. The current study addresses the prevalence of these issues.

Psychological Use

In addition to the practical usage of ICTs and SNSs, literature has also examined the psychological use and effects associated with radicalization and Internet usage (Brachman 2006; Freiburger and Crane 2008; Jenkins 2011; Silber and Bhatt 2007). The emergent theme from this literature conveys the notion that the Internet is a powerful developmental tool, which can be used by terrorists to spread ideology and propaganda quickly and effectively, while reaching and influencing aggrieved sympathizers by using multiple learning models (Freiburger and Craine 2008; O'Shaughnessy and Baines 2009). Most important, evidence shows that Internet propaganda, along with other tools, can be used to imbue vulnerable individuals, who may be experiencing feelings of alienation or marginalization as well as personal and group grievances, with radical narrative, making them more susceptible to perpetrating acts of expressive violence (Bartlett, Birdwell, and King 2010; Silber and Bhatt 2007).

Clearly, the story is more complicated, and its completeness has been hampered by a general lack of terrorism data, as it relates to Internet usage. The current study provides and assesses comprehensive terrorism data on the roles of usage and its impact on the overall process of radicalization. In sum, terrorism research may need to assess organizing threat and mobility differently. Collective action has been changed and now extends into the placeless environment that contains all the practical and psychological tools beneficial to any business, organization, or

movement. The ability of ICTs and SNSs to radicalize, empower, and mobilize followers of terrorist movements cannot be ignored. With the ever-expanding capabilities of these technologies, these movements can clearly benefit from developments in research, training, communication, and recruitment. Nevertheless, the prior research claims about the prevalence, types, and purposes of Internet use within domestic terrorist plots within the United States need to be assessed empirically.

Theory and Evidence Overview

To empirically examine the prevalence, type, and purpose of ICT usage among these movements requires an understanding of why characteristic group differences in ICT usage might exist beyond the individual composition of movement membership. Given that both the personal circumstances of individuals combined with social structure seem to drive use overall (Selwyn et al., 2005), it seems likely that demographic, ideological, and cultural factors all coalesce in shaping ICT use among terrorists.

Among the general population, ICTs are mainly used as a means of communication and a way to highlight news and information (Cole, 2008; Hlebec et al., 2006). SNSs are primarily used as a form of expression for those who prefer not to socialize face-to-face (Tufekci, 2008). Overall, income seems to drive ICT use among industrialized nations (Chinn and Fairlie, 2007; OECD, 2001; US Department of Commerce, 2002); nevertheless, at the macro-level, not only income, but regulatory effectiveness, telecommunications infrastructure, and human capital drive use of ICTs (Chinn and Fairlie, 2007; Dasgupta, 2001; Wallsten, 2005). Beyond this, there has been a need to examine cultural factors in addressing the use and adoption of technology (Bagozzi, 2007; Gretzel, Myughwa, and Lee, 2008; Okazaki, 2005). Culture plays an important role in the way both individuals and groups adopt technology (Anandarajan, Igbaria, and

Anakwe, 2002; Ein-Dor, Segev, and Orgad, 1993; Kumar, Ganesh, and Echambadi, 1998; Rogers and Shoemaker, 1971; Schepers and Wetzels, 2007; Straub, Keil, and Brenner, 1997; Takada and Jain, 1991), specifically ICTs (Pavlou and Fygenson, 2006). Overall, U.S. consumers spend more time on the Internet and more time creating content than any of their counterparts (Gretzel, Myughwa, and Lee, 2008). Just as culture plays an important role in the adoption of ICTs in certain countries, the same may be true within terrorist movements. Low-context cultures such as the U.S. differ from high-context, collectivist cultures in terms of their communication needs and styles (Gretzel, Myughwa, and Lee, 2008); therefore, although differing in many respects, it is likely that Western culture predominantly affects the needs and motives for ICT use/adoption among movements operating within the United States. The practical and culturally driven needs for ICT usage among the general population allow for a deeper understanding of how these factors combine with individual characteristics of users, thus producing differences in ICT use across terrorist movements.

Contribution of Research

Accordingly, the current analysis possesses myriad practical implications for counter-radicalization and counterintelligence strategies, as well as academic research and public policy initiatives. The next section briefly discusses the merits and contributions to both the governmental and nongovernmental field of research on online radicalization to violent extremism in the United States. The data currently available from the American Terrorism Study (ATS) (i.e. Smith and Damphousse 2013) should assist to remedy the lack of empirical work in two ways. First, this project should facilitate the delineation of the impact and difference of types and purposes of ICT use among these three movements during pre-incident activity, as well as within the process of radicalization leading to violent extremism. Second, it will systematically

examine demographics of individual and movement members among Internet users and nonusers, potentially creating a typology to compare to the general population of the United States. The ATS database allows for the study of persons indicted at the federal level for official acts of terrorism and terrorism-related charges from 1980 through 2012. For this specific analysis, from 1995-2011, these court cases provide a population of over 320 indictees for an exploratory study of Internet usage, frequency of use, type of use, and purpose of use in the pre-incident planning processes, as well as individual background information.

The results from this study may have significant impacts both on policy and practice. Unlike traditional criminal behavior, terrorism occurs over long periods of time, across multiple geographic units, involving complicated social networks with both direct and indirect contact, among persons engaging in numerous pre-incident activities. Inherently, the Internet has perceivably both changed and enhanced these processes. The results from this analysis will assist both the practitioner and policymaker to better understand the process of Internet usage within domestic terrorist plots in the United States. This analysis explores new ground in quantifying practical and psychological types of Internet use; there are few if any studies that have attempted to quantify the process within the context of domestic terrorism using these specific constructs.

At present, there is no single study that has quantified and/or examined the pattern of Internet usage among domestic terrorists or terrorist movements. It is the goal of this study to not only put use/non-use in the context of how domestic terrorists compare to the general population, but also how those patterns are different across three major terrorist movements. The current research maintains that while much of the focus of law enforcement and intelligence agencies has been on the online activities of Islamic extremist movements, other terrorist movements have been using the Internet and social media to communicate with one another. A more

comprehensive approach to analyzing this data between movements should be of great benefit to those agencies wanting to know more about the who, what, where and how of radicalization and pre-incident planning facilitated by the Internet.

It has been established that Islamic extremist movements are using ICTs and SNSs for many of the aforementioned purposes; however, it has not been established whether or not uses such as these are prevalent among other movements, or how prevalent they are within Islamic extremist movements. Measuring types and purposes of use, combined with individual and group correlates of users and nonusers will allow for a more comprehensive understanding of this phenomenon as it occurs within different terrorist movements. The following analysis provides and assesses comprehensive terrorism data on the roles of ICT usage within the pre-incident planning process of domestic terrorists. In addition, the analysis both attempts to answer and raise certain questions pertaining to the threat of online self-radicalization occurring in the United States. In sum, terrorism research needs to assess organizing threat and mobility differently. With ICTs, the dynamics of collective action have perceivably been changed and now extend into the placeless environment that contains all the practical and psychological tools beneficial to any business, organization, or movement. The ability of ICTs and SNSs to radicalize, empower, and mobilize followers of terrorist movements cannot be ignored; however, prevalence of threat has never been quantitatively assessed. With the ever-expanding capabilities of these technologies, these movements may clearly benefit from developments in research, training, communication, and recruitment.

Data and Methods

To address each of the separate issues previously raised in literature on users/nonusers of ICTs and terroristic use of the Internet within the pre-incident planning process, the present analysis uses court documents and other open-source documentation from "officially designated" Federal terrorism court cases pertaining to movements operating in the United States (Smith et al., 2006; Smith et al., 2008). Documents from each of the federal terrorism cases are maintained as part of the American Terrorism Study (ATS). The ATS dataset currently contains information on nearly 4,000 precursor activities related to 437 incidents and planned incidents from 1971 to 2013. Information over 400 variables from these cases have been extracted from the court records and quantified for empirical analyses.

It has been established that terrorism requires more extensive preparation than that of traditional criminality (Smith et al., 2006; 2008). This planning process has been streamlined by ICTs, and recruitment appears to have been enhanced by online social media (Brachman, 2006; O'neil and Gray, 2011; Saeed, Rohde, and Wulf, 2008; Thompson, 2011). The variables pertaining to these issues were related to the use of ICTs within the pre-incident planning process among environmental, far-right, and Islamic extremist movements. In addition, quantitative measures of type and purpose of ICT use, as well as the background characteristics of users/nonusers were established to quantify correlates and variation in the aforementioned measures within and between ideological movements.

Measurement

Use and Demographics

The current project focuses only on the years 1995-2011. The Internet officially became "commercial" in 1995 with the advent of Internet Service Providers (ISP's). Therefore, this exploratory analysis focused not only on the first decade of the 21st century, but when the Internet came onto the commercial market. Thus, the present analysis extracted information for all known terrorist incident plots with a conviction (court case) since 1995 (n = 149). The ATS data reveal that multiple actors were involved in both plots and incidents as reflected in the indictments and open-source documentation. Therefore, demographic information on all known persons indicted in each incident plot and act (indictees) (n = 331) were collected as demographic measures, which include the following: *Age* (1 = 1, 99 = 99 years of age); *Sex* (0 = female); *Race* (0 = white); *Marital Status* (0 = married); and *Education* (0 = less than high school). *Use* is also an independent measure *User*/*Nonuser* (0 = User) to establish demographic correlates of ICT *Use*.

It should be noted that this measurement does not include individual "co-conspirators" who were allegedly involved in the plot but were not indicted. All court cases selected represent terrorist plots where an incident act was carried-out, whether successful or failed. The court cases and individuals were then assigned to categories or *movements* representing the associated terrorist movement name or ideology in association with a specific terrorist incident: (case study) (n = 86).

Variation between Terrorist Movements

Next, the differences in both ICT use and demographics between terrorist movements were examined with (1) the independent measure of *Terrorist Movement* (1 = environmental, 2 =

far-right, and 3 = Islamic extremist); and (2) the dependent measure of variation of *use* (0 = Yes) between terrorist movement. Demographic correlates of *User/Nonuser* (0 = User) and the variation across movements were then examined: *Age* (1 = 1, 99 = 99 years of age), *Sex* (0 = female), *Race* (0 = white); *Marital Status* (0 = married), *Education* (0 = less than high school), and *Terrorist Movement* (1 = environmental, 2 = far-right, and 3 = Islamic extremist). In addition, *Use* (0 = Yes) was used as a measure of the overall prevalence of ICT use among movements.

These variables allow for the creation of measures and examination of: 1) the overall prevalence of *Use* across terrorist movements; 2) the variation of the *Demographics* across terrorist movements; and 3) the variation of *Use* across terrorist movements.

Terrorist Use by Prevalence, Type, and Purpose

After establishing measures of prevalence, demographic correlates, and variance among those correlates across movements, a dependent measure of *Use Type* (1 = information gathering, 2 = distribution of propaganda, 3 = communication, 4 = planning and coordination, 5 = information sharing, 6 = claiming responsibility for attacks, 7 = training, 8 = target selection, 9 = website creation, 10 = cyber-attacks, 11 = publicity, 12 = the radicalization of civilians, 13 = terroristic threatening, 14 = recruitment, 15 = fund raising, 16 = performance analysis, 17 = disinformation, 18 = remote attack, 19 = information security, or 20 = use of the internet as a tool for inspiration/indoctrination) within and between movements was used to assess the most prevalent type of ICT usage and whether *Use Type* varied significantly across terrorist movements.

These comparisons allowed for demographic and typological measures that can be compared to correlates of Use and Type of Use across the general non-terrorist population,

further expanding the breadth of knowledge about special populations of terrorists and associated movements.

Estimating Internet Usage

The last segment of the analysis offers two logistic regression models measuring the likelihood of various factors predicting odds of usage. The independent demographic measures *Age* (1 = 1, 99 = 99 years of age), *Sex* (0 = female), *Race* (0 = white); and *Marital Status* (0 = married) and the independent measure of *Terrorist Movement* (0 Islamic extremist, 1 = environmental, 2 = far-right) were used in these exploratory models.

As a result, the present analysis focuses on **four primary questions/issues**: 1) Demographic correlates of Internet users and nonusers from the terrorist sample in relationship to the general population; 2) A description of type of Internet usage for the entire terrorist sample; 3) The differences in Internet usage across the three terrorist movements (environmental, far-right, and Islamic extremist); and 4) The differences in types and purposes of Internet usage across these movements.

Analytic Framework

The current analysis begins with an examination of the demographics and overall prevalence of Internet use between movements. This allowed for the first quantitative analysis of variance of ICT use among environmental, far-right, and Islamic terrorist movements within the pre-incident planning process. Given that these three emergent terrorist threats varied demographically, it also allowed for a comparison of the demographics of "users" and "nonusers" to the research findings on those correlates among the general population. Given the differences emergent between movements, an analysis of variance among users and nonusers was then employed to assess both how ICT use varies across movements, and how demographics

vary across movements. Reviewing the extant literature on terrorist use of the Internet created the more complicated question about how and what terrorists are using ICTs. Therefore, two binomial logistic regression models were used to assess terrorist demographics across movement to determine what demographics drive Internet usage, as well as to explain differences in use and type of use across terrorist movement.

Results

Descriptive Statistics

To begin with, over the 16-year period examined in the present analysis, over half (55%) of the cases that were prosecuted were found to contain clear evidence of ICT usage related to the incident (either preparatory or target specific). Table 1 provides measures of the prevalence of Internet use, demographics, group types, as well as how ICTs were used during the planning process of domestic terrorist plots in the United States from 1995 to 2011. In the case of "claiming responsibility" for an attack, this generally occurred after the incident was carried out, though in some cases the communiqués were started before the incident was carried out. For the entire sample (n = 331), the average age of movement members was 35 years old. Affirming previous research on terrorist demographics, the majority of members were married (47%), white (68%) males (86%) possessing more than a high school education (68%) with very few (3.5%) having less than a high school education. The categories representing the terrorist movements examined–environmental (30%), far-right (35%), and Islamic extremist (34%)–were relatively proportionate across the sample. Additionally, while not shown in the tables, it was found that eighty-three percent of Islamic extremist were ICT users, followed by environmental (51%) and

Table 1. Descriptive Statistics for Demographics & Model Variables (n = 331)			
Dependent Variable	%	Mean	S.D.
Use	55.30%		
Demographics			
Age		34.62	13.539
Sex (0 = Male)	86.20%		
Race (0 = White)	67.80%		
Marital (0 = Married)	47.10%		
Education (0 = Less than HS)	3.50%		
Movement			
Environmental	30.51%		
User %	51.49%		
Far-Right	35.05%		
User %	31.03%		
Islamic Extremist	34.44%		
User %	83.33%		
Types of Use			
Communication	42.90%		
Info Gathering	35.60%		
Propaganda	32.30%		
Planning	15.40%		
Train	13.30%		
Info Sharing	12.10%		
Claim	12.10%		
Publicity	9.70%		
Threatening	8.20%		
Web Creation	6.60%		
Recruitment	6.00%		
Target	3.30%		
Cyber-Attack	2.10%		
Radicalization	1.80%		

far-right (31%). For all movements, communication (43%) was the most common use during the planning process, followed by information gathering (36%) and propaganda (32%). Overall, it appears that far-right movements used ICTs far less than both Islamic and environmental movements, while Islamic and environmental movements have similar frequencies of usage generally. Clearly, domestic terrorist movements used the Internet extensively for practical or strategic purposes during the planning process. Table 2 provides measures of the demographic and category differences between users and nonusers for the entire sample (n = 331). There was no significant difference in age between users (35) and nonusers (35). Overall, the demographics of ICT users from the entire sample were much like the general demographics for all terrorists, making it hard to infer a specific "typology." Users were most likely to be white (26%) males (49%) who were married (29%) and well educated (44%). Race, gender, and educational attainment coincide with findings among ICTs in the general population; however, unlike general population demographics, age was not a good predictor of ICT usage in the sample. Therefore, it was found that some of the same predictors of ICT use among the general population may not apply to the sample terrorist population. Of the movements represented, the analysis again illustrates Islamic extremists (29%) were the heaviest users as a movement within the entire sample, followed by environmental (15%) and then far-right (11%). The percentage measures of use and nonuse across demographics and within each of the categories of terrorist movements is also listed.

Table 3 depicts the differences in types of use between terrorist movement types. Within those who used ICTs, Islamic extremists used more than other movements for communication (60%), information gathering (64%), distributing propaganda (54%), and planning (53%). Cramer's V was exceptionally strong between movement types, information gathering, and

communication. These results are in accordance with the extensive qualitative work on potential terrorist uses of Internet by Islamic extremists (Freiburger and Crane, 2008; Jenkins, 2010, 2011; UNODC, 2012; Theohary and Rollins, 2011; Weimann, 2004, 2005, 2010, 2011, 2012;)However, within those that used the Internet during the incident planning process, environmental movements used ICTs more than Islamic extremists for recruiting (100%), information sharing (60%), training (54%), and radicalization (67%). Aside from domestic recruitment of members in the U.S., which occurred strictly within environmental movements, Islamic extremists still maintained a prevalence of ICT use for training (45%), information sharing (17%), and radicalization (33%) that was significantly lower than that of environmental movements. Finally, and also unique to environmental movements, ICTs were being used to claim responsibility for attacks (100%) and using the Internet for cyber-attacks (100%). Although not always occurring specifically within the pre-incident planning process–although some of these ELF/ALF communiqués were started before an incident–this use of media is still an important representation of how movements might use ICTs to further their cause. All of these findings were statistically significant (Chi-Square) except for radicalization.

Table 4 provides the binomial logistic regression results estimating ICT usage. For model 1, despite the descriptive statistics showing that the age of terrorist movement Internet users and nonusers was not statistically significant, the results of the regression analysis show that ICTs users were more likely to be younger. In addition, users are less likely to be females, five times more likely to be white, and almost 3 times more likely to be married. However, only race is significant. After introducing the terrorist movement types in model 2, I see that the age is no longer significant in the model. This supports the previous findings that the age between terrorist users and nonusers is not a good predictor of ICT use. The explained variance in model 2 is

Table 2. Demographics and Movement Differences Between Users and Nonusers (n = 331)

	Use	Nonuse	%	X^2	p.
Demographics					
$\bar{X}$ *Age*	34.69	34.55			0.921
Sex				0.471	0.492
Male	159 (48.80%)	122 (37.40%)	13.80%		
% within use/nonuse	87.40%	84.70%			
Female	23 (7.10%)	22 (6.70%)	86.20%		
% within use/nonuse	12.60%	15.30%			
Race				38.581	0.001
White	93 (29.30%)	122 (38.50%)	67.80%		
% within use/nonuse	53.10%	85.90%			
Nonwhite	82 (25.90%)	20 (6.30%)	32.20%		
% within use/nonuse	46.90%	14.10%			
Education				4.747	0.093
Less than HS	5 (3.50%)	0 (0.00%)	3.50%		
% within use/nonuse	5.70%	0%			
HS	21 (14.80%)	19 (13.40%)	28.20%		
% within use/nonuse	23.90%	35.20%			
More than HS	62 (43.70%)	35 (24.60%)	68.30%		
% within use/nonuse	70.50%	64.80%			
Marital				3.799	0.15
Married	49 (28.50%)	32 (18.60%)	47.10%		
% within use/nonuse	49.00%	44.40%			
Single	40 (23.30%)	37 (21.50%)	23.30%		
% within use/nonuse	40.00%	51.40%			
Other	11 (6.4%)	3 (1.70%)	8.10%		
% within use/nonuse	11.00%	4.20%			
Movement				64.465	0.001
Environmental	52 (15.70%)	49 (14.80%)	30.51%		
% within use/nonuse	28.40%	31.30%			
Far-Right	36 (10.90%)	80 (24.20%)	35.04%		
% within use/nonuse	19.70%	54.10%			
Islamic Extremist	95 (28.70%)	19 (5.70%)	34.44%		
% within use/nonuse	51.90%	12.80%			

Table 3. Use Type Differences Between Terrorist Movements (n = 331)

Use Type	Use	%/Use	Nonuse	%/Nonuse	X2	p.	Cramer's V
Communication					82.62	0.000	0.5
Environmental	36 (10.90%)	25.40%	65 (19.60%)	34.40%			
Far-Right	20 (6.00%)	14.10%	96 (29.00%)	50.80%			
Islamic	86 (26.00%)	60.60%	28 (8.50%)	14.80%			
Info Gathering					76.91	0.000	0.48
Environmental	30 (9.10%)	25.40%	71 (21.50%)	33.30%			
Far-Right	13 (3.90%)	11.00%	103 (31.10%)	48.40%			
Islamic	75 (22.70%)	63.60%	39 (11.80%)	18.30%			
Propaganda					44.41	0.000	0.36
Environmental	37 (11.20%)	34.60%	64 (19.30%)	28.60%			
Far-Right	12 (3.60%	11.20%	104 (31.40%)	46.40%			
Islamic	58 (17.50%)	54.20%	56 (16.90%)	25.00%			
Planning					32.53	0.000	0.31
Environmental	24 (7.30%)	47.10%	77 (23.30%)	27.50%			
Far-Right	--		116 (35.00%)	41.40%			
Islamic	27 (8.20%)	52.90%	87 (26.30%)	31.10%			
Train					29.18	0.000	0.30
Environmental	24 (7.30%)	54.50%	77 (23.30%)	26.80%			
Far-Right	--		116 (35.00%)	40.40%			
Islamic	20 (6.00%)	45.50%	94 (28.40%)	32.80%			
Info Sharing					18.8	0.000	0.24
Environmental	24 (7.30%)	60.00%	77 (23.30%)	26.50%			
Far-Right	9 (2.70%)	22.50%	107 (32.30%)	36.80%			
Islamic	7 (2.10%)	17.50%	107 (32.30%)	36.80%			
Claim					103.61	0.000	0.56
Environmental	40 (12.10%)	100.00%	61 (18.40%)	21.10%			
Far-Right	--		116 (35.0%)	39.90%			
Islamic	--		114 (34.40%)	39.20%			
Target					6.54	0.038	0.14
Environmental	6 (1.80%)	54.50%	95 (28.70%)	29.70%			
Far-Right	--		116 (35.00%)	36.20%			
Islamic	5 (1.50%)	45.50%	109 (32.90%)	34.10%			
Recruitment					48.47	0.000	0.38
Environmental	20 (6.00%)	100.00%	81 (24.50%)	26.00%			
Far-Right	--	37.30%	116 (35.00%)				
Islamic	--	36.70%	114 (34.40%)				
Cyber-Attack							
Environmental	7 (2.10%)	100.00%	94 (28.40%)	29.00%	16.29	0.000	0.22
Far-Right	--		116 (35.00%)	35.80%			
Islamic	--		114 (34.40%)	35.20%			
Radicalization					4.76	0.092	0.12
Environmental	4 (1.20%)	66.70%	97 (29.30%)	29.80%			
Far-Right	--		116 (35.00%)	35.70%			
Islamic	2 (.60%)	33.30%	112 (33.80%)	34.50%			

Table 4. Logistic Regression Models Estimating Internet Usage (n = 331)

	Model 1	O.R.	Model 2	O.R.
Age	-0.008	0.992	0.006	1.006
Sex	-0.631	0.532	-0.377	0.686
Race	1.681	5.315	0.527	1.693
Mstat				
Mstat 1	-0.057	0.945	-0.322	0.725
Mstat 2	1.011	2.749	0.958	2.605
Islamic				
Environmental			-0.461	0.631
Far-Right			-1.678	0.187
Constant	0.685		1.261	
DF	5		7	
R-Squared (Nagelkerke)	0.164		0.227	

Reference Categories: Islamic Extremist, Female, Less Than High School, Married, White

increased from 16 to 23 percent. Again, after controlling for all other variables, users are less likely to be female, almost two times more likely to be white, and almost three times more likely to be married. However race is not significant in model 2. Finally, the results show that while environmental terrorist are not significantly different than Islamic extremists in ICT usage, there is a statistically significant difference between Islamic extremists and the far-right movements with far-right terrorists using ICT significantly less than Islamic extremists. Clearly, these movements have differences and this preliminary analysis points to some important findings worthy of more detailed analyses that is beyond the scope of the present paper.

Discussion

Little evidence of self-radicalization or recruitment occurring online among Islamic extremists was found within this particular sample. In fact, using ICTs to recruit members domestically appeared to be most prominent among environmental movements. In addition, no strategic use of social networking sites (SNSs) among Islamic extremists was found. Again, the only evidence of strategic use of SNSs was recorded among environmental terrorists. It appears that, at least in terms of domestic terrorism, these uses are not as prevalent as what might have been assumed. As suggested earlier, the majority of information was taken from the FBI investigations and there is the potential that the ICT use was either well hidden, undetected, or not pertinent to establishing probable cause in an indictment. Such activity may have occurred but it was simply not mentioned in any court documents.

As indicated, ICTs are prevalently used by terrorist movements for reasons practical to their unique operational and ideological needs. Islamic extremists recorded the most prevalence in ICT usage. Nevertheless, many of the usage forms often associated with Islamic movements, were found to be more closely associated with environmental movements in this analysis. This underscores the point that not all terrorist movements are alike in terms of ICT usage, among other factors, and should not be lumped into a single category. Consequently, this brings into light the overshadowing focus on Islamic threats, as well as the importance of understanding what differences drive ICT usage–and other planning activities for that matter–across movements and why. The significant differences in ICT use among these terrorist movements exposed are likely driven by the exclusive characteristics and needs of each movement. Furthermore, while the demographics of older, less educated far-right members who used less in

the overall sample coincide with the demographic correlates among the general population of nonusers, the story is clearly more complicated.

Overall, the demographic correlates of ICT users were difficult to separate from both nonusers and the entire sample of terrorists. This makes it difficult to infer any specific typology of an ICT "user" or "nonuser" other than middle-aged, white, married, well-educated male profile typical of the findings pertaining to the majority of terrorists in general. The age of user and nonusers being relatively the same illustrates the point that while organizational and philosophical needs may drive different operational planning strategies, terrorists in general may be similar in various ways, such as demographics, yet much different from the general or criminal population. Furthermore, even though the majority of users were white, that percentage was not much more than nonwhite users. Likewise, within users and nonusers, although ICT users were slightly more educated, nonusers were also highly educated. This further supports the research findings that terrorists differ from the general and/or criminal population in terms of demographics. Married individuals are more likely to use, but yet again, that percentage is only slightly higher than singles, making it difficult to infer specific predictors. Ultimately, analysis of a larger population of terrorists is needed to further assess demographics in relationship to ICT usage.

Although occurring with slightly less frequency, the same practical needs seem to also drive ICT use among environmental terrorists for communication, information gathering, the distribution of propaganda, and planning. Nevertheless, environmental movements take prevalence over Islamic and far-right movements for the rest of the use type variables: training, information sharing, target selection, recruitment, cyber-attacks, threatening, web-creation, publicity, and radicalization. It should be noted that several of these use types–claiming

responsibility, website-creation, recruitment, and cyber-attacks–were unique to environmental cases in this study. In the sample, twice as many individuals were radicalized, three times as many individuals were sharing information, and seven times as many individuals were using ICTs to gain publicity than Islamic extremists as were used by environmental movements. Although the "ELF Family" was systematically dismantled by criminal agency investigations in the late 90s and early 2000s, it is clear that this movement and associated environmental movements have set a precedent of ways to operate using ICTs (Smith and Damphousse 2009). While the focus has been mainly upon movements like Al-Qa'ida, specific movements may adopt ICT use to meet the particular needs of the movement. Their strong Internet presence may again reflect their organizational constraints or needs. Although far-right users were less prevalent in most cases, it should be again noted that the far-right leaderless resistance was organized around the idea of using ICTs to facilitate protection of movement leaders from civil and criminal liability (Beam, 1992; Kaplan, 1997). Far-right use for communication was comparable to environmental movements. Their information sharing was equivalent to that of Islamic extremists. Finally, the far-right used the Internet more for both threatening and publicity than Islamic extremists. It is distinctly evident that these movements use the Internet differently.

Finally, just as demographic differences dictate the opportunity to access and skills to operate ICTs, the same may hold true for macro-level differences. The diverse backgrounds of individuals comprising the aforementioned movements, combined with the varying background characteristics of the movements themselves, may work confluent in producing outcomes in ICT usage. Beyond the practicality of culturally driven needs of communication and news/information sharing, the general public's drive to use ICTs for social interaction and escape make them formidable psychological tools to reach vulnerable populations; however, little

evidence of this was found. Nevertheless, as research expands, demographics may partly determine which individuals are online for indoctrination, to be recruited, or even radicalized. Such constraints may likely translate into certain populations perceiving online propaganda as culturally resonant, and accordingly those populations may be targeted. As the IT-driven era and information age continue to expand, the attributes and attraction of seemingly troubled individuals to these technologies may proffer the expansion of ICT use among individuals experiencing grievances, terrorists seeking to reach those experiencing those grievances, or simply networking to spread ideology or recruit.

Conclusion

Although little evidence of online radicalization or self-radicalization was found, the precedent set by environmental movements and their ICT usage emphasizes that the Internet and associated technologies cannot be discounted as viable terrorist tools. Practically, ICTs are clearly tools and extensions of social movements, their operations, and their ideologies. ICTs are an integral part of the pre-incident planning process, assessing information and sharing it. Moving into and through an IT-driven era, reliance on such technological tools is likely to become more prevalent for social groups and movements in the future. Currently, social scientists have a unique opportunity to study the convergence of our social world with these technologies. The fact that Al-Qa'ida and Islamic extremists have overshadowed public and government concern about other movements attests to the social construction of terrorism in the United States after 9/11. Clearly, other terrorist threats have remained prominent but out of the media and public sphere's concern. The other movements in this study are clearly different from Islamic extremists in terms of their use, their message, and their organizational needs.

Accordingly, other movements have the same opportunity to use ICTs and models for such usage have been set by groups such as environmental movements.

Finally, this study should bring to light many questions as to how terrorists, at least domestically, are currently using ICTs to plan terrorist incidents and the threats associated with such use. As society as a whole becomes more reliant on ICTs, social scientists have a responsibility to assess and measure both its social uses and effects. While use for socializing and radicalizing individuals online remains a threat, the results from this analysis stress the need to understand the fundamental needs and philosophies behind terrorist movements, how they differ, and how these differences translate in to different uses of ICTs as social tools to advance their causes. The threat clearly comes from practical, everyday use, and at least for now, it appears that socialization and radicalization of terrorist movement members still occurs in groups with the facilitation and indoctrination of other group members.

References

Aerschot, Lina V. and Rodousakis, Niki. 2008. "The Link Between Socio-economic Background And Internet Use: Barriers Faced By Low Socio-economic Status Groups And Possible Solutions." *Innovation: The European Journal of Social Science Research*. 21(4): 317-351.

Anandarajan, M., Igbaria, M., and Anakwe, U. P. 2002. "IT acceptance in a less-developed country: A motivational factor perspective." *International Journal of Information Management*, 22(1): 47-65.

Bagozzi, R. 2007. "The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift." *Journal of the Association for Information Systems*, 8(4): 244-254.

Bartlett, Jamie, Birdwell, Jonathon, and King, Michael. 2010. E*dge of Violence: A Radical Approach to Extremism*. London, Demos.

Bergen, Peter, Hoffman, Bruce, and Tiedemann, Katherine. 2011. "Assessing the Jihadist Terrorist Threat to American and American Interests. *Studies in Conflict & Terrorism.* 34(2):65-101.

Brachman, Jarret. M. 2006. "High-tech terror: Al-Qaeda's use of new technology." Manuscript submitted for publication, Combating Terrorism Center, United States Military Academy, Lincoln Hall, New York.

Beaudon, Christopher, E. 2008. "The Internet's Impact on International Knowledge." *New Media & Society*. 10(3): 455-474.

Brandtzaeg, Petter, B. 2012. "Social Networking Sites: Their Users and Social Implications – A Longitudinal Study." *Journal of Computer-Mediated Communication.* 17: 467-488.

Buffardi, Laura E., & Campbell, W. Keith. 2008. "Narcissism and social networking web sites." *Personality and Social Psychology Bulletin, 34:* 1303-1314.

Chen, Yiwei and Persson, Anna. 2002. "Internet Use Among Young and Older Adults: Relation to Psychological Well-Being." *Educational Gerontology*. 28: 731-744.

Chinn, Menzie, D. and Fairlie, Robert W. 2007. "The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration." *Oxford Economic Papers.* 59: 16-44.

Coetzee, Liezl. 2008. "World Wide Webs: Social Movements Cross Global Divides in the Public Cyber-Sphere. *Science, Technology, and Society in Africa.* 4(1):80-94.

Cole, Jeffrey. 2004. "Now Is the Time to Start Studying the Internet Age." *Chronicles of Higher Education.* 50(30): 1-4.

Czaja, Sara J. and Lee, Chin Chin. 2007. "The Impact of Aging on Access to Technology." *Universal Access in the Information Society.* 5: 341-349.

Dasgupta, S., Lall, S., and Wheeler, D. 2001. "Policy Reform, Economic Growth and the Digital Divide: An Econometric Analysis." Working Paper No. 2567 (World Bank).

Dholakia, R. R. 2006. Gender and IT in the Household: Evolving Patterns of Internet Use in the United States. *Information Society*, 22(4): 231-240.

Dijk, Jan van and Hacker, 2003. "The digital divide as a complex and dynamic phenomenon," *Information Society*, (19)4: 315–326.

Earl, Jennifer S. and Rohlinger, Deana. 2012. *Media, Movements, and Political Change.* Bingley, UK: Emerald Group Publishing.

Ein-Dor, P., Segev, E., and Orgad, M. 1993. The Effect of National Culture on IS: Implications for International Information Systems. *Journal of Global Information Management.* 1(1): 33-44.

Flanagan, Andrew J. and Metzger, Miriam J. 2001."Internet Use in the Contemporary Media Environment." *Human Communication Research.* 27(1): 153-181.

Floridi, Luciano. 2007. "A Look in the Future Impact of ICT on Our Lives." *The Information Society.* 23: 59-64.

Fitzpatrick, Kevin., Smith, Brent L., Roberts, Paxton., and Damphousse, Kelly. 2013. "Does Context Matter? Exploring the Role of Community in Understanding Terrorist Pre-Incident Activity in the United States, 1990-2010." *Unpublished manuscript.*

Freiburger, Tina., and Crane, Jeffrey S., 2008. "A Systematic Examination of Terrorist Use of the Internet." *International Journal of Cyber Criminology*, 2(1): 309-319.

Friedland, Jamie and Rogerson, Kenneth. 2009. "How Political and Social Movements Form on the Internet and How They Change Over Time." *Literature Review.* Institute for Homeland Security Solutions.

Freilich, Joshua D., Steven M. Chermak, Roberta Belli, Jeff Gruenewald, and William S. Parkin. 2014. "Introducing the United States Extremist Crime Database (ECDB)." *Terrorism & Political Violence*, 26(2): In press.

Gaibulloev, Khusrav., Sandler, Todd., and Santifort, Charlinda. 2012. "Assessing the Evolving Threat of Terrorism." *Global Policy.* 3(2):135-144.

Gangadharbatla, Harsha. 2008. Facebook Me: Collective Self-Esteem, Need to Belong, and Internet Self-Efficacy as Predictors of the Internet Generation's Attitudes Toward Social Networking Sites." *Journal of Interactive advertising.* 8(2): 1–28.

Garret, R. K. 2006. “Protest in an Information Society: A Review of Literature on Social Movements and New ICTs. *Information, Communication and Society.* 9(2):202-224.

Gillet, J. 2003. “Media Activism and Internet use by people with HIV/AIDS.” *Sociology of Health & Illness.* 25(6): 608-624.

Grace-Farfaglia, Patricia, Dekkers, Ad, Sundararajan, Binod, Peters, Lois, and Park, Sung-Hee. 2006. “Multinational Web Uses and Gratifications: Measuring the Social Impact of Online Community Participation across National Boundaries. *Electronic Commerce Research.* 6(75): 75-101.

Gretzel, Ulrike, Myunghwa, Kang and Lee, Woojin. 2008. “Differences in Consumer-Generated Media Adoption and Use: A Cross-National Perspective.” *Journal of Hospitality & Leisure Marketing.* 17(1-2): 99-120.

Haythornthwaite, Caroline. 2005. “Social Networks and Internet Connectivity Effects.” *Information, Communication & Society.* 8(2): 125-147.

Hlebec, Valentina, Manfreda, Katja L. and Vehovar, Vasja. 2006. “The Socio Support Networks of Internet Users.” *New Media & Society.* 8(1): 9-32.

Jenkins, Brian M. 2007. “Building an Army of Believers: Jihadist Radicalization and Recruitment.” Testimonial, RAND Corporation.

Jenkins, Brian Michael. 2010. “Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States September 11, 2001.” Testimonial, RAND Corporation.

Jenkins, Brian Michael. 2011. “Jihadist Use of Social Media—How to Prevent Terrorism and Preserve Innovation.” Testimonial, Committee on Homeland Security and House of Representatives.

Jenkins, Brian Michael. 2011. “Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11.” Testimonial, RAND Corporation.

Joosse, Paul. 2007. “Leaderless Resistance and Ideological Inclusion: The Case of the Earth Liberation Front.” Terrorism and Political Violence. 19(3):351-368.

Institute for Strategic Dialogue. 2011. “Radicalization: The Role of the Internet. A Working Paper of the PPN.” 48 Charles Street, London.

Klausen, Jytte, Barbieri, Elaine T., Reichlin-Melnick, Aaron, and Zelin, Aaron Y. 2012. The YouTube Jihadists: A Social Network Analysis of Al-Muhajiroun’s Propaganda Campaign. *Perspectives on Terrorism.* 6(1)

Korkeila, J., Kaarlas, S. Jaaskelainen, M., Vahlberg, T. and Taiminen, T. 2010. "Attached to the Web – Harmful Use of the Internet and its Correlates." *European Psychiatry.* 25: 236-241.

Kraut, Robert, Patterson, Michael, Lundmark, Kiesler, Sara, Mukopadhyay, Tridas and Scherlis, William. 1998. "Internet Paradox. A Social Technology that Reduces Social Involvement and Psychological Well-being?" *American Psychology.* 53(9): 1017-1031.

Kwon, Nahyun and Zweizig, Douglas L. 2006. "Use of Community Information and Communication Technologies (ICTs): Explaining the Use of Community Networks with Demographic Factors, Psychological Factors, and Alternative Service Accessibility." *The Library Quarterly.* 76(1): 81-106.

Kumar, V., Ganesh, Jaishankar, and Echambadi, Raj. 1998. "Cross-National Diffusion Research: What We Know and How Certain Are We?" *The Journal of Product Innovation Management.*15(3): 255-268.

LaFree, Gary, and Bianca Bersani. *Hot Spots of Terrorism and Other Crimes in the United States, 1970 to 2008*. Final Report to Human Factors/Behavioral Sciences Division, Science and Technology Directorate, U.S. Department of Homeland Security.

Leader, Sefan F. and Probst, Peter. 2003. "The Earth Liberation Front and Environmental Terrorism. *Terrorism and Political Violence.* 15(4):37-58.

Lee, Nam-Jin, Shah, Dhavan V., & McLeod, Jack. M. 2012. "Process of political socialization: A communication mediation approach to youth civic engagement." *Communication Research*. 1-29.

Mehdizadeh, Soraya. 2010. "Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook." *CyberPsychology, Behavior & Social Networking.* 13(4): 357.

Moussa, Mohamed B. 2011. "The Use of the Internet by Islamic Social Movements in Collective Action: The Case of Justice and Charity." *Westminister Papers in Communication and Culture.* 8(2):154-177.

Myrick, Sue., Thompson, Mike., Gannon, John C., and Nuemann, Peter. 2011. "Preventing Violent Radicalization in America." House Permanent Select Committee on Intelligence Subcommittee on Terrorism, HUMINT, Analysis, and Counterintelligence, July 27th 2011.

Nambayah, Mani and Quickenden. 2004. "A Quantitative Assessment of Chemical Techniques for Detecting Traces of Explosive at Counter-Terrorist Portals." *Talanta.* 63(2):461-467.

Norris, Pippa.2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge, Cambridge University Press.

OECD. 2001. “Understanding the Digital Divide.” (Paris: Organization for Economic Cooperation and Development).

O’shaughnessy, Nicholas J. and Baines, Paul R. 2009. “Selling Terror: The Symbolisation and Positioning of Jihad.” *Marketing Theory.* 9(2): 227-241.

O’Neil, Michael. and Gray, David H. 2011. “Islamic Terror Networks Implementation of Network Technologies.” *Global Security Studies.* 2(3): 41-51.

Okazaki, S. 2005. “New Perspectives on M-Commerce Research.” *Journal of Electronic Commerce Research,* 6(3): 160- 165.

Olesen, Thomas. 2009. “Islamism as Social Movement.” *Centre for Studies in Islamism and Radicalization (CIR).* Department of Political Science, Aarhus University, Denmark.

Organization for Security and Co-operation in Europe (OSCE). 2008. “Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation.” *Second International Forum on Information Security.* Garmisch-Partenkirchen, 7-10 April.

Ong, Chorng-Shyong, Chang, Shu-Chen and Wang, Chih-Chien. 2011. “Comparative Loneliness of Users Versus Nonusers of Online Chatting.” *Cyberpsychology, Behavior, and Social Networking.* 14(1-2): 35-40.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and Prediction Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. MIS Quarterly, 30(1), 115-143.

Pollet, Thomas V., Roberts, Sam G.B., and Dunbar, Robin I.M. 2011. “Use of Social Network Sites and Instant Messaging Does Not Lead to Increased Offline Social Network Size, or to Emotionally Closer Relationships with Offline Network Members.” *Cyberpsychology, Behavior, and Social Networking.* 14(4): 253-258.

Quibria, M. G., Shamsun N. Ahmed, Ted Tschang, and Mari-Len Reyes-Macasaquit. 2002. "Digital divide: Determinants and policies with special reference to Asia." Economics and Research Department Working Paper No. 27 (Manila: Asia Development Bank).

Ressler, Steve. 2006. “Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research.” *Homeland Security Affairs.* 2(2):1-10.

Roe, Keith. and Broos, Agnetha. 2005. “Marginality in the Information Society: The Socio-Demographics of Computer Disquietude.” *Communications: The European Journal of Communications.* 30(1): 91-96.

Robinson, John P. and Martin, Steven. 2009. “IT and Activity Displacement: Behavioral Evidence from the U.S. General Social Survey (GSS). *Social Indicators Research.* 91(2): 115-139.

Rogers, E. M. and Shoemaker, F. F. 1971. *Communication of Innovations: A Cross-Cultural Approach.* New York: Free Press.

Perry, Ronald W. 2003. "Incident Management Systems in Disaster Management." *Disaster Prevention and Management.* 12(5):405-412.

Ryan, Tracii and Xenos, Sophia. 2011. "Who Uses Facebook? An Investigation into the Relationship Between the Big Five, Shyness, Narcissism, Loneliness, and Facebook Usage." *Computers in Human Behavior.* 27: 1658-1664.

Saeed, Saqib, Rohde, Markus and Wulf, Voker. 2008. "ICT's, an Alternative Sphere for Social Movements in Pakistan – A Research Framework." *Department of Information Systems and New Media.* University of Seigen, Holderlinstr, Germany.

Schepers, J. & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: investigating subjective norm and moderation effects. Information & Management, 44, 90-103.

Selwyn, N., Gorard, S., and Furlong, J. 2005. "Whose Internet is it Anyways? Exploring Adults' (Non)Use of the Internet in Everyday Life. *European Journal of Communication.* 20(1): 5-6.

Selwyn, N, Gorard, S, & Furlong, J 2006. *Adult Learning in the Digital Age*, Routledge: London.

Shangapour, Soran, Hosseini, Seidawan , and Hashemnejad, Hashem. 2011. Cyber social-networks and social movements Case study: Tehran (2009-10). *International Journal of Scientific & Engineering Research.* 2(1):1-12.

Sheldon, Pavica. 2012. "Profiling the Non-Users: Examination of Life-Position Indicators, Sensation Seeking, Shyness, and Loneliness Among Users and Non-Users of Social Network Sites." *Computers and Human Behavior.* 28: 1960-1965.

Shu, Wesley and Chuang, Yu-Hao. 2011. "The Perceived Benefits of Six-Degree-Separation Social Networks." *Internet Research.* 21(1): 26-45.

Silber, Mitchell D. and Bhatt, Arvin. 2007. "Radicalization in the West: The Homegrown Threat." *Report, New York Police Department Intelligence Division.*

Silke, Andrew. 2008. "Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalization." *European Journal of Criminology,* 5(1): 99-123.

Slater, Matthew S. and Trunkey, Donald D. 1997. "Terrorism in American: An Evolving Threat." *Archives of Surgery.* 132(10):1059-1066.

Smith, Brent L., and Morgan, Kathryn D. 1994. Terrorists Right and Left: Empirical Issues in Profiling American Terrorists. *Studies in Conflict and Terrorism,* 1:39-57 UK: Taylor & Francis.

Smith, Brent L., and Damphousse, Kelly R. 2009. “Patterns of Precursor Behaviors in the Life Span of a U.S. Environmental Terrorist Group.” *Criminology & Public Policy* 8:3.

Smith, Brent L., Damphousse, Kelly R., and Roberts, Paxton. 2006. “Pre-Incident Indicators of Terrorist Incidents: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct.” National Institute of Justice.

Smith, Brent L., Cothren, Jackson., Roberts, Paxton., and Damphousse, Kelly R. 2006. “Geospatial Analysis of Terrorist Activities: The Identification of Spatial and Temporal Patterns of Preparatory Behavior of International and Environmental Terrorists.” Department of Justice.

Southern Poverty Law Center 2009. “The Second Wave: Return of the Militias.” Retrieved August 12, 2009, from http://www.splcenter.org/images/dynamic/main/The_Second_Wave.pdf

Steinmuller, W. Edward, 2001. "ICTs and the Possibilities of Leapfrogging by Developing Countries." *International Labour Review*, 140(2): 193-210.

Straub, D., Keil, M., & Brenner, W. 1997. “Testing the Technology Acceptance Model Across Cultures: A Three Country Study.” *Information and Management*, 33(1): 1-11.

Takada, H. and Jain, D. 1991. “Cross-National Analysis of Diffusion of Consumer Durable Goods in Pacific Rim Countries*.” Journal of Marketing*, 55: 48-54.

Theohary, Catherine A., and Rollins, John. 2011. “Terrorist Use of the Internet: Information Operations in Cyberspace. Retrieved from www.fas.org Jan 7, 2013 (http://www.fas.org/sgp/crs/terror/R41674.pdf)

Thompson, Robin. 2011. “Radicalization and the Use of Social Media.” *Journal of Strategic Security.* 4(4): 167-190.

Tufekci, Z. 2008. “Grooming, Gossip, Facebook and MySpace: What Can We Learn about these sites from those who won’t assimilate?” *Information, Communication & Society*, 11(4): 544–564.

United Nations Office on Drugs and Crime, In collaboration with United Nations Counter-Terrorism Implementation Task Force (UNODC). 2012. “The use of the Internet for terrorist purposes.” United Nations, Office at Vienna.Weimann, Gabriel. 2004. "www.terror.net How Modern Terrorist Use The internet." *United States Institute of Peace*. Washington D.C. Retrieved from www.usip.org on Jan 7, 2013 (http://www.usip.org/files/resources/sr116.pdf).

U.S. Department of Commerce. 2000. “Falling Through the Net: Toward Digital Inclusion.” (Washington, DC: U.S. GPO).

U.S. Executive Office of the President. 2011. Empowering Local Partners to Prevent Violent Extremism in the United States. Washington, D.C.: White House.

U.S. Executive Office of the President. 2011. Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States. Washington, D.C.: White House.

Verdegem, Pieter and Verhoest, Pascal. 2009. "Profiling the Non-User: Rethinking Policy Initiatives Stimulating ICT Acceptance." *Telecommunications Policy.* 33: 642-652.

Wallsten, Scott J. 2005. "Regulation and Internet Use in Developing Countries." *Economic Development and Cultural Change*. 53(2): 501-523.

Weiman, Gabriel. 2005. "How Modern Terrorist Use the Internet." *The Journal of International Security Affairs.*

Weimann, Gabriel. 2010. "Terror on Facebook, Twitter, YouTube." *Brown Journal of World Affairs,* 16(1): 45-54.

Weimann, Gabriel. 2011. "Al Qaeda Has Sent You a Friend Request: Terrorists Using Online Social Networking." Manuscript submitted for publication, Communication, Haifa University, Israel.

Weimann, Gabriel. 2012. "Lone Wolves in Cyberspace." *Journal of Terrorism Research.* 3(2).

Meehan, Patrick., McCants, William., Weisburd, A. Aaron., Jenkins, Brian. and Kohlmann, Evan F. 2011. "Jihadist Use of Social Media – How to Prevent Terrorism and Preserve Innovation." House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence, December 6th.

Youmans, William L. and York, Jillian C. 2012. "Social Media and the Activist Toolkit: User Agreements, Corporate Interests, and the Information Infrastructure of Modern Social. *Journal of Communication.* 62:315-329.

Zickuhr, Kathryn. 2010. "Generations 2010." *Pew Research Center*: Washington D.C. Retrieved from www.pewinternet.org on November 15, 2013 (http://www.pewinternet.org/~/media/Files/Reports/2010/PIP_Generations_and_Tech10.pdf)

March 24, 2014

MEMORANDUM

TO:	Brent Smith David Woodring Kevin Fitzpatrick
FROM:	Ro Windwalker IRB Coordinator
RE:	New Protocol Approval
IRB Protocol #:	14-03-521
Protocol Title:	*21st Century Radicalization: The Role of the Internet User and Nonuser in Terroristic Outcomes*
Review Type:	☒ EXEMPT ☐ EXPEDITED ☐ FULL IRB
Approved Project Period:	Start Date: 03/24/2014 Expiration Date: 03/23/2015

Your protocol has been approved by the IRB. Protocols are approved for a maximum period of one year. If you wish to continue the project past the approved project period (see above), you must submit a request, using the form *Continuing Review for IRB Approved Projects*, prior to the expiration date. This form is available from the IRB Coordinator or on the Research Compliance website (http://vpred.uark.edu/210.php). As a courtesy, you will be sent a reminder two months in advance of that date. However, failure to receive a reminder does not negate your obligation to make the request in sufficient time for review and approval. Federal regulations prohibit retroactive approval of continuation. Failure to receive approval to continue the project prior to the expiration date will result in Termination of the protocol approval. The IRB Coordinator can give you guidance on submission times.

If you wish to make *any* modifications in the approved protocol, you must seek approval *prior to* implementing those changes. All modifications should be requested in writing (email is acceptable) and must provide sufficient detail to assess the impact of the change.

If you have questions or need any assistance from the IRB, please contact me at 210 Administration Building, 5-2208, or irb@uark.edu