1-1-2016

Terrorist Experts' Perceptions of How the Internet Has Shaped International Terrorism

Samuel F. Wilson II
Walden University

Teresa M. Lao Ph.D.
Walden University, teresa.lao@waldenu.edu

Ernesto Escobedo Dr.
Walden University, ernesto.escobedo@waldenu.edu

2016

Terrorist Experts' Perceptions of How the Internet Has Shaped International Terrorism

Samuel F. Wilson II
Walden University

Teresa M. Lao Ph.D.
Walden University

Ernesto Escobedo Dr.
Walden University

IBIMA Publishing
Journal of Information Assurance & Cyber security
http://www.ibimapublishing.com/journals/JIACS/jiacs.html
Vol. 2016 (2016), Article ID 163033, 20 pages
DOI: 10.5171/2016.163033

Research Article

Terrorist Experts' Perceptions of How the Internet Has Shaped International Terrorism

Samuel F. Wilson II[1], Teresa M. Lao[2] and Ernesto Escobedo[3]

[1]Walden University, 6972 Village Stream Place, Gainesville

[2]Walden University, 15602 Ruidosa Canyon, Helotes, TX

[3]Walden University, 17606 King Corner Street, San Antonio, TX

Correspondence should be addressed to: Samuel F. Wilson II; samuel.wilson@waldenu.edu

Received date: 29 February 2016; Accepted date: 13 June 2016; Published date: 21 September 2016

Academic Editor: Jivika Govil

Abstract

The use of the Internet by terrorists has greatly contributed to international terrorism. The Internet is a main strategic communication asset for terrorists who use online message boards and chat rooms to share information, coordinate attacks, spread propaganda, raise money, and recruit. The Internet gives terrorists a medium to legitimize, propagate, and intimidate citizens to their cause. Their strategies are based on careful analysis of human communications; thus, messages are adapted and carefully delivered to appeal to people who may need something to believe in. This study bridged the gap in knowledge by exploring, understanding, and explaining the perceptions of 10 American terrorist experts on how the use of the Internet by terrorists has shaped international terrorism. Findings of the study indicate that the use of the Internet by terrorists has shaped international terrorism, which resulted in major challenges for counterterrorism agencies in the United States and abroad due to the ability of terrorists to easily close, change, and create new websites or accounts. In addition, counterterrorism experts also have to deal with advanced encryption software and the anonymity of terrorist suspects. Terrorists are able to attract other like-minded individuals or sympathizers to their cause by using the Internet as the medium of communication. The research is significant in that it is directed at the U.S. intelligence community and international counterterrorism entities in order to make continuous improvements in the United States' homeland security by recognizing terrorist Internet tactics so they can quickly and effectively respond to them. This requires collaboration among counterterrorism agencies and organizations in the U.S. as well as collaboration among member states.

Keywords: Terrorism, international terrorism, propaganda, Internet tactics, counterterrorism

Cite this Article as: Samuel F. Wilson II, Teresa M. Lao and Ernesto Escobedo (2016), "Terrorist Experts' Perceptions of How the Internet Has Shaped International Terrorism", Journal of Information Assurance & Cyber security, Vol. 2016 (2016), Article ID 163033, DOI: 10.5171/2016. 163033

Introduction

Terrorism is a relevant issue in today's globalized society. Technology has made it easier and faster for individuals to access information around the world. Individuals could easily get information about terrorist attacks, recruitment, and terrorism in general via the Internet. Should someone from outside the United States decide to recruit or influence those who live in the U.S., they could easily do so by sending a message on the World Wide Web. For radicals, the Internet is a valuable tool used to strengthen their cause (Soriano, 2012). As a tool, the Internet provides extremists with the ability to collaborate and inspire others to take up their cause, where some then carry out terrorist attacks independently (Soriano, 2012).

In response to the September 11, 2001 terrorist attacks (9/11) and other terrorist threats in the United States, the counterterrorism agencies and organizations have taken steps against al-Qa'ida, the transnational terrorist organization that is responsible for planning and conducting the attacks (The White House, 2011). For this study, when the word terrorists is used, this term will pertain to individuals who use "force or violence against persons or property in violation of the criminal laws of the United States for purposes of intimidation, coercion, or ransom" (Federal Emergency Management Agency [FEMA], 2013, p. 148). With the establishment of the Internet, terrorists now use it to disseminate information, both near and far, with efforts to recruit members (Stern, 1999). According to Kaplan (2009), there are over 5,000 jihadi websites; however, less than 100 of these are monitored by Pentagon analysts. An essential component of Internet recruitment is social media, which consists of e-mail, egroups, and message boards (Weismann, 2010). The message board is a connector for potential terrorist agents and communication can be as simple as generating a quick response or providing elaborate memos (Weismann).

In fighting against terrorism, the UNODC (2012) reported that the Internet has created both challenges and opportunities. Therefore, with the increasing use of the Internet for terrorist purposes, a proactive and coordinated response by member states is needed. According to The White House (2011), President Obama's National Strategy for Counterterrorism focuses on disrupting, dismantling, and defeating al-Qa'ida, its affiliates, and adherents to ensure the security of the American people and its interests.

The purpose of this phenomenological research study was to bridge the gap in knowledge by exploring, understanding, and explaining the perceptions of 10 American terrorist experts on how the use of the Internet by terrorists has shaped international terrorism. Subsequently, the implications for positive social change stemming from this study are directed toward the U.S. intelligence community, which includes 17 agencies and organizations such as the Department of Homeland Security (DHS), Federal Bureau of Investigations (FBI), Central Intelligence Agency (CIA), National Geospatial-Intelligence Agency (NGA), and the Office of the Director of National Intelligence (ODNI). In addition, implications are also directed toward the Counter-Terrorism Implementation Task Force (CTITF) that consists of 31 international entities such as the United Nations System in Counter-Terrorism Efforts Organigram, as a proactive and coordinated response by member states was recommended by the UNODC (2012). The findings from the study are applicable to many agencies and organizations and a wide array of fields, to include public policy and administration, emergency management, criminal justice, criminal law, and criminal psychology.

Background

The Internet is a powerful vehicle of communication for business, education, healthcare, politics, and terrorism. Because

Samuel F. Wilson II, Teresa M. Lao and Ernesto Escobedo (2016), Journal of Information Assurance & Cybersecurity, DOI: 10.5171/2016. 163033

communication on the Internet does not necessarily get filtered for any types of terrorist recruitment, there is an immediate cause of concern as to what messages are being transmitted by outside groups residing in other countries other than the US. We need to be alarmed of this ongoing threat because the Internet has emerged as an instrumental tool for terrorist planning, facilitation, and communication, which offers terrorists several advantages (Mount Holyoke College, 2014; The White House, 2011). Through the use of the Internet, terrorists are able to operate remotely and anonymously without being detected or regulated. People living in the United States may not also be tracked for their possible involvement or willingness to respond to terrorist recruitment. Someone who may be going to US college may be an unsuspecting recruit for terrorist activities (Mount Holyoke College, 2014).

According to the United Nations Interregional Crime and Justice Research Institute (2014), terrorists established a presence on the Internet through official terrorist websites run by terrorist organizations or extremist religious scholars, unofficial terrorist websites such as discussion forums and blogs, and distributor websites such as online magazines and videos. Terrorists use the Internet to spread their propaganda, which includes recruitment, radicalization, and incitement to terrorism (United Nations Office of Drugs and Crime, 2012).

Because little is known on how international terrorism is being organized today, this phenomenological study could bridge the gap in knowledge by exploring, understanding, and explaining the perceptions of 10 American terrorist experts on how the use of the Internet by terrorists may have shaped international terrorism.

Access to Technology and Information

Because of the immediate availability of the Internet to anyone in the world who has access to a computer, terrorist organizations no longer face a learning curve in accessing and delivering information online (Hedges, 2008). In fact, the most inexperienced and underfunded terrorist now has the potential to carry out attacks due to the detailed experiences and lessons posted online.

Hedges (2008) noted that today's terrorism is a manifestation of an evolution of asymmetric conflict that has existed from the beginning of time. Therefore, terrorists' use of the Internet should be treated and analyzed like other tactical innovations in order to understand how it affects terrorist behavior and how it makes them vulnerable. Hence, while it is important to know how the Internet helps terrorists, it is also important to understand and recognize the weaknesses that accompany its use, which is important in the development of counterterrorism policies (Hedges, 2008; Heickerö, 2008).

As Hedges (2008) noted, similar to terrorists learning from one another, so too, can counterterrorism agencies and organizations. Counterterrorism agencies and organizations should recognize that terrorists' use of the Internet has both costs and benefits that are inherent in its use. As policymakers and practitioners, counterterrorism agencies and organizations should not ignore the limitations of the Internet, but should recognize the opponents' tactics and quickly and effectively respond to them. This is imperative to the national security of the United States and other countries, thus saving the lives of the American people and first responders and adding to the effort to make continuous improvements in the nation's homeland security.

Research pertaining to online terrorist recruitment has indicated the challenges associated with this use of the Internet technology (Hedges, 2008; Heickerö, 2008; Kaplan, 2009; UNODC, 2012). Terrorist groups have become more adaptive and have used the Internet to achieve support for their cause (Lubold, 2010). Gohel (2009) reported that extremists can be recruited and become involved in terrorist plots through

anonymous contacts. The Internet has become a catalyst for spreading messages of violence and attracting sympathizers. Jazib (2010) related that the Internet is now the main tool used by terrorists to locate resources and spread ideas, thus accelerating radicalization. Therefore, terrorists' use of the Internet should be treated and analyzed like other tactical innovations in order to understand how it affects terrorist behavior and how it makes them vulnerable. Hence, while it is important to know how the Internet helps terrorists, it is also important to understand and recognize the weaknesses that accompany its use, which is important in the development of counterterrorism policies (Hedges, 2008; Heickerö, 2008).

Problem

The United States' most preeminent security threat continues to be from al-Qa'ida, its affiliates, and adherents (The White House, 2011). Mass media and the Internet have emerged as enablers for terrorist planning, facilitation, and communication (Hedges, 2008; Heickerö, 2008; Kaplan, 2009; UNODC, 2012; The White House, 2011). The use of the Internet allows terrorists to operate without the confines of borders and increases the potential impact on victims (UNODC, 2012).

Researchers of online terrorist recruitment have noted the challenges associated with this use of the Internet technology (Hedges, 2008; Heickerö, 2008; Kaplan, 2009; UNODC, 2012). Terrorist groups have become more adaptive and have used the Internet to achieve support for their cause (Lubold, 2010). Gohel (2009) reported that extremists can be recruited and become involved in terrorist plots through anonymous contacts.
While it is important to know how the Internet helps terrorists, it is also important to understand and recognize the weaknesses that accompany its use, which is important in the development of counterterrorism policies (Hedges, 2008; Heickerö, 2008). Due to the significance of the use of the Internet by terrorists, this phenomenological research study can help bridge the gap in knowledge by exploring, understanding, and explaining the perceptions of 10 American terrorist experts on how the use of the Internet by terrorists has shaped international terrorism is needed.

To address the issue concerning international terrorism, this phenomenological study addressed one central research question: How has the use of the Internet by terrorists shaped international terrorism?

Five subquestions were considered:
1. What Internet strategies of recruitment are used by terrorist organizations?
2. In what ways are terrorist Internet recruitment efforts supported by the United States?
3. What measures are in place to counter online terrorist recruitment efforts?
4. In what direction is terrorist recruitment heading?
5. How is online terrorist recruitment evolving in the 21st century?

Theoretical Framework

Stepanova's (2008) asymmetric conflict theory served as the theoretical framework of this study. Asymmetric conflict or warfare is described as "a conflict in which the resources of two belligerents differ in essence and in the struggle, interact and attempt to exploit each other's characteristic weaknesses" (Princeton University, 2014, para. 2). The struggle often involves strategies and tactics of unconventional warfare, where the weaker combatant attempts to use strategies to offset its deficiencies in quantity or quality (Princeton University, 2014). According
to Stepanova (2008), nation-states have continuing conventional superiority in regards to power and status over nonstate actors. However, terrorist groups have many comparative advantages in their confrontation with states due to their extremist ideologies and dispersed organizational structures. Therefore, weaker

opponents are able to defeat strong adversaries because of their use of powerful tools (Roberts, 2000; Stepanova, 2008).

Scholars have noted terrorism to be an example of asymmetric conflict, in which terrorist organizations are the weaker adversaries (Mount Holyoke College, 2014). According to Mount Holyoke College (2014), terrorists use inferior resources against the weaknesses of the superior opponent. Terrorists are small substate actors who have less power than nation-states that they are fighting against. This forces this group to use unorthodox means to achieve their goals.

According to Mount Holyoke College (2014), terrorists use inferior resources against the weaknesses of the superior opponent. Terrorists are small substate actors who have less power than nation-states that they are fighting against. This therefore forces them to use unorthodox means to achieve their goals. On the other hand, unlike nation-states, terrorists have the option to remain completely anonymous until they commit an act of terror. They have developed skills in operating from remote locations, avoiding detection by law enforcement surveillance, and evading designated security checkpoints (Theohary & Rollins, 2011). Hence, terrorists use their differences to compensate for their disadvantages against nation-states (Mount Holyoke College, 2014). Mount Holyoke College (2014) related that asymmetric tools used by terrorists include crashing airplanes into the World Trade Center and sending out anthrax-laced mail in order to further their objectives despite their inferior power. In addition, using the Internet is another asymmetric tool used by terrorists.

Terrorists' Use of the Internet

The development of the Internet can be traced back to 1957 when the Soviet Union launched the Sputnik satellite, which was the world's first manmade satellite into orbit (A&E Television Networks, 2014; George Mason University History News Network, 2014). As a result, the Advanced Research Projects Agency (ARPA) was established in 1958 to research and develop new technology for the United States military. Since the late 1980s, the Internet has been a dynamic means of communication worldwide (UNODC, 2012). With the establishment of the Internet, terrorists now use it to disseminate information, both near and far, with efforts to recruit members (Stern, 1999). Stern (1999) related that the communication barrier that geography once presented to radical groups has now been overcome by today's advanced online technology.

Information about Terrorist Websites

According to Kaplan (2009), there are over 5,000 jihadi websites; however, less than 100 of these are monitored by Pentagon analysts. Terrorist websites include official site of terrorist organizations and websites of supporters, sympathizers, and fans (Weimann, 2006). Defining some websites as terrorist websites is unclear when the websites have no formal terrorist affiliation (Kaplan, 2009). Terrorist monitors may also find it challenging to monitor hoax sites due to frequent site outages. In addition, there are 11 known terrorist chat rooms (Weimann 2013).

Extremists come from all ethnic, racial, and cultural backgrounds (Spargo, 2007). A major concern is the vast presence of extremist groups online (Conway 2007). A contributing factor for this growth is the ease of website development (Freiburger & Crane, 2008). Other major concerns include access availability, limited regulation, and the speed in which a message can be transmitted (Weimann & Von Knop, 2008). Websites can be set up any time by registering a universal resource locator (URL) and providing identifying data such as a name, address, and primary means of contact (Hoffman, 1996). Once a website is operational, the content is available to Internet users around the globe (Shetret, 2011). According to Gray and Head (2009), that translates to approximately 20% of people around the world or at least 1.3

billion individuals as of 2008. The researchers noted that although affluent countries typically have the greatest number of users, both Africa and the Middle East have seen increased use of the Internet by over 900% in the past eight years.

An essential component of Internet recruitment is social media, which consists of e-mail, egroups, and message boards (Weimann, 2010). The message board is a connector for potential terrorist agents and communication can be as simple as generating a quick response or providing elaborate memos (Weismann, 2010). Forest (2006) provided a segment of a conversation that took place in an al-Qa'ida chat room, which highlighted an application called Pal Talk which allows terrorists to communicate without detection. Weimann (2010) restated that extremists use chat rooms in order to receive guidance, information, and instructions. For example, Kershaw (2004) noted that Army National Guardsman Ryan Anderson converted to Islam after visiting Islamic websites and used the name Amir Abdul Rashad. The researcher reported that Anderson revealed military information to an undercover federal agent whom he thought was a terrorist operative.

Thomas (2003) reported that terrorists use the Internet to provide a sense of constant support to potential followers (Thomas, 2003). Websites are accessible at any time and provide insight into various topics of interest. Information on firearms, virtual training camps, strategic communicators, and operation planning and coordination instructions are all readily available (Gray & Head, 2009).

Social networks such as Facebook and Twitter are also instrumental in recruitment (Wiemann, 2010). Such sites enable web surfers to give and receive instant messages and photos (Wiemann, 2010). Caldwell (2008) related that the strategies used by extremist organizations are similar to those used by other corporations. This may be magnified by the advanced recruitment methods that are used by al-Qa'ida to include video recording to display their messages, CD-ROMS which contains data, and recorded cassettes, all of which provide an opportunity for recruits to receive information and to get the message to multiple followers (Forest, 2006). For example, Jackson (2007) discussed an on-line video where terrorists were shown assembling a suicide belt.

Another noteworthy aspect of Internet recruitment is the ability to tap into conventional media sources (Denning, 2009). Denning (2009) indicated that these sources include newspapers, television broadcasts, and radio. For example, jihadist websites have disseminated information and resources to potential recruits in the form of electronic magazines and supplemental digital videos related to television audio recordings of jihadist leaders. Hummel (2008) discussed digital video examples such as the murder and beheading of Daniel Pearlman and Nick Berg, 9/11, and vehicle borne improvised explosive device attacks against U.S Forces in Iraq and Afghanistan. Homeland Security Institute (2009) presented videos of an incident involving young people in the United Kingdom who filmed themselves reenacting beheadings. Therefore, youths were copying videos of beheadings, which were posted online by terrorist groups or their supporters.

Terrorist Internet Strategies of Recruitment

Theohary and Rollins (2011) reported that websites provide the capability to publicize, raise awareness, and to attract potential followers. The extremist sites are used as a communication method to unite, interact, arrange, and carry out missions (Brown & Korff, 2009). The UNODC (2012) identified six ways in which the Internet is utilized for terrorist purposes: (a) propaganda, (b) financing, (c) training, (d) planning, (e) execution, and (f) cyberattacks.

Propaganda

Propaganda includes recruitment, radicalization, and incitement to terrorism (UNODC, 2012). The UNODC (2012) noted that dissemination of propaganda is one of the main uses of the Internet by terrorists. This is done through multimedia communications where ideological or practical instructions are provided, explanations, justifications, or the promotion of terrorist activities. Furthermore, this may include information developed by terrorist organizations and sympathizers, such as virtual messages, presentations, magazines, treatises, audio and video files, and video games.

However, what is described as propaganda can be subjective since a basic tenet of international law is the right to freedom of expression (UNODC, 2012). Individuals have the right to share their opinion or distribute content even if it is objectionable to others; however, there are some limited exceptions. These exceptions include the distribution of certain sexual explicit content and communications detrimental to the protection of national security and communications (UNODC).

According to Radlauer (2013), a sense of belonging is important to human beings. The Internet is an avenue to reach out and recruit those that might be open to the terrorist's message (Lewis, 2005). According to Wright (2008), radicals frequently seek out individuals who feel alone or frustrated, offering them a sense of belonging. This feeling of inclusion appears to be a prominent feature in the ability to recruit online.

In recruiting, terrorists must tap into their target audiences (Schmidle, 2009). Schmidle (2009) stated that extremists gain support by showing validity in their cause. Support is partly gained by showing pictures depicting the enemy administering harm to terrorist groups, women, children, or sympathizers (Tsfati & Weimann, 2002). Terrorists are not just adults and they work to inspire the younger generation to take part in their movement (Tsfati & Weimann, 2002). Singer (2012) reported that almost every young man or woman have access to a computer. Homeland Security Institute (2009) noted several accounts of Islamic Jihad and Hamas recruiting 13-year-old teens for suicide bomb missions and children 11 years old trafficking weapons and explosives. For example, two sisters recruited and linked to al-Qa'ida were filmed in an attempt to demolish business and government buildings.

Financing

Acts of terrorism are financed by terrorist organizations and supporters through the use of the Internet (UNODC, 2012). According to the UNODC (2012), four categories are used to describe the manner in which terrorists use the Internet to raise and collect funds and resources: (a) direct solicitation, (b) e-commerce, (c) exploitation of online payment tools, and (d) through charitable organizations. Direct solicitation pertains to the request for donations from supporters through the use of websites, chat groups, mass mailings, and targeted communications. In regards to e-commerce, supporters may be offered books, audio and video recordings, and other items at online stores. In regards to the exploitation of online payment tools, it is easy to transfer funds electronically between parties due to the dedicated websites and communication platforms. In addition, fraud may occur with online payment facilities, such as identity and credit card theft; wire, stock, and auction fraud; and intellectual property crime. In regards to charitable organizations, individuals may provide financial support to what appears to be legitimate charitable organization and the funds may be used for terrorist purposes. Therefore, terrorist organizations may establish shell corporations to obtain online donations.

Training

The Internet is increasingly being used as an alternative training ground or virtual training camp for terrorists (UNODC, 2012). Both alternate training ground and virtual training camps provide terrorist groups a greater opportunity to distribute their messages. Internet training enhances followers' ability to execute the operational tools to carry out the mission (Gaibulloev & Sadler, 2013). Similarly, many terrorist organizations use video cameras to highlight their operations for potential followers (Michael, 2013).

Execution

The UNODC (2012) reported that elements from propaganda, financing, training, and planning may be used in the execution of terrorist acts. For example, the Internet may be used to disseminate explicit threats of violence in order to cause anxiety, fear, or panic among a targeted population. Such threats may be deemed unlawful by many member states, even if the threats are not carried out. The use of the Internet decreases the chances of being detected and helps to hide the identity of those responsible for terrorist acts. Therefore, terrorist organizations' dissemination explicits threats under different aliases to protect their identity (Soriano, 2013).

Measures to Counter Online Terrorist Recruitment

In fighting against terrorism, the UNODC (2012) reported that the Internet has created both challenges and opportunities. Therefore, with the increasing use of the Internet for terrorist purposes, a proactive and coordinated response by member states is needed. The UNODC noted that despite the international recognition of the terrorist Internet threat, there is currently no universal instrument that specifically addresses this aspect of terrorist activity. In addition, specialized training is limited on the legal and practical aspects of the investigation and prosecution of terrorist cases involving the use of the Internet.

There is a wealth of information on how jihadist groups utilize the Internet to spread propaganda, communicate with distant cells, and organize attacks (Hedges, 2008). However, research has been sparse on how the use of the Internet by terrorists has shaped international terrorism (Hedges, 2008). Therefore, this phenomenological research study bridged the gap in knowledge by exploring, understanding, and explaining the perceptions of American terrorist experts on how the use of the Internet by terrorists has shaped international terrorism.

Discussion

Data analysis for this study consisted of thematic analysis and constant comparison from in-depth open-ended interviews and e-mail questionnaires. The NVivo software facilitated the identification of themes and provided annotation for the codes and categories.

Instrumentation and Data Collection

In-depth semistructured interviews served as the main data collection instrument for this study in order to obtain the perceptions of 10 American terrorist experts on how the use of the Internet by terrorists has shaped international terrorism. The interviews consisted of five questions that were developed to answer the central research question and five subquestions. Based on participants' location and availability, two participants participated in face-to-face interviews, one participated by telephone, and seven participated by e-mail. All participants were American citizens, with eight residing in the United States and two residing overseas.

Procedures

In the beginning, 60 potential participants who met the study's criteria were e-mailed an invitation letter to participate in the study.

Any questions that the potential participants had were answered. From the 60 experts who were contacted, 17 agreed to participate in the study. However, seven individuals were unable to take part due to their organizations' privacy policies; therefore, 10 individuals participated in the study.

The participants included eight males and two females. Eight resided in the United States and two resided overseas. Participants worked in the fields of homeland security (two professors), law enforcement, government, criminal justice, psychology, communication, and IT. Participants' held bachelor's, master's, and doctoral degrees. Therefore, diverse perspectives on the topic of study were sought from individuals who had investigated, studied, taught, and reported on terrorists' use of the Internet. The demographic breakdown appears in Table 1.

Table 1: Basic Demographics of the Participants in the Study

Participants	Gender	Education	Field	Location
Participant 1	Male	Masters	Communication	United States
Participant 2	Male	Bachelors	Law Enforcement	United States
Participant 3	Male	Bachelors	Government	United States
Participant 4	Male	Masters	IT	United States
Participant 5	Male	PhD	Law Enforcement	United States
Participant 6	Male	PhD	Government	United States
Participant 7	Male	JD	Communication	United States
Participant 8	Female	PhD	Homeland Security	Overseas
Participant 9	Female	PhD	Homeland Security	Overseas
Participant 10	Male	PhD & MD	Psychology	United States

Note. IT = Information Technology.

The 10 participants were e-mailed a consent form, which they electronically signed and returned. After receiving the electronically signed consent form from each participant, each participant was contacted by phone or e-mail to set-up a 60-minute appointment for individual semistructured interviews at a time and place that was convenient for them. Based on participants' location and availability, two participants participated in face-to-face interviews, one participated by telephone, and seven participated by e-mail. Face-to-face and telephone interviews were audio-taped and took approximately 60 minutes. Individuals who participated by e-mail completed the e-mail questionnaire and e-mailed me their responses. Before concluding the face-to-face and telephone interviews, participants were asked if they have any other questions or concerns. After addressing any questions or concerns, the interviews were concluded and participants were thanked for their participation.

Based on participants' location and availability, two participants participated in face-to-face interviews, one participated by telephone, and seven participated by completing an e-mail questionnaire (see Table 2). Face-to-face and telephone interviews were audio-taped and took approximately 60 minutes. Individuals who participated by e-mail completed the

questionnaire and e-mailed me their responses.

Table 2: Data Collection Method

Participants	Face-to-Face	Telephone	E-mail
Participant 1			X
Participant 2	X		
Participant 3	X		
Participant 4			X
Participant 5			X
Participant 6			X
Participant 7			X
Participant 8			X
Participant 9			X
Participant 10		X	

Data Analysis Plan

Qualitative data were analyzed the seven steps of the modified van Kaam method of analysis of phenomenological data (Moustakas, 1994, pp. 120-121), which is discussed in detail further in the paper. Moustakas (1994) emphasized the significance of identifying pertinent statements for analysis. Data from the in-depth face-to-face and telephone interviews and e-mail questionnaires were coded, NVivo data analysis software was used to organize and analyze the data. NVivo assisted with data analysis, which is to interpret the research findings after describing the sample and their behavior (Creswell, 2010). Coding and categorization of interviews facilitated thematic analysis of data. The NVivo software facilitated the identification of themes and provided annotation for the codes and categories. The themes were modified and broken down into subthemes. Coding followed a prespecified protocol based upon key words such as *international terrorism*, *recruitment strategies*, *recruitment efforts*, and *counterterrorism*.

Participation in the study did not cause any acute discomfort. Being in the study did not pose risk to their safety or well-being. After the data were collected, all identifiable data were eliminated; therefore, the interviews were numbered or coded in order to match each participant, thus protecting participants' identity. Participants were informed that the interviews would be audio-taped and that a verbatim transcription would be made and analyzed later. All audio-recorded data were kept secured and transcribed.

The analysis of data collected was crucial to finding meaning within the phenomenon

studied. See Appendix A for the Microsoft Excel spreadsheet of the thematic analysis step 2 or the exploration of text. The results present each major theme and important experiences, which were supported by verbatim passages from participants. This section is organized in the following subsections: thematic analysis and results.

Thematic Analysis

The modified van Kaam method of analysis of phenomenological data (Moustakas, 1994, pp. 120-121) was used. This subsection is organized in the following areas: reduction and elimination, clustering and thematizing, final identification of themes, individual textural descriptions, individual structural descriptions, individual composite descriptions, and composite textural-structural descriptions.

Reductions and Elimination

According to Moustakas (1994), the first step of the modified van Kaam method is the listing and preliminary grouping of the answers of the participants, which is also known as the horizonalization process. This first step was performed when I listed all perceptions shared by the participants that were vital to the phenomenon being explored in the study. The second process, known as the reduction and elimination step, was arranged according to two questions to discern whether the responses of the participants should be incorporated in the next stages of the study or eliminated early on (Moustakas, 1994, p. 121): (a) Does it contain a moment of the experience that is necessary and sufficient for understanding it and (b) is it possible to abstract and label it? If so, it was a horizon of the experience. An expression not meeting the above requirements was eliminated. Overlapping, repetitive, and vague expressions were also eliminated or presented in more descriptive terms. The horizons that remained were the themes of the experience.

Clustering and thematizing. The other most important experiences that were formed from the second step of the method were gathered and clustered together to establish thematic labels (Moustakas, 1994). These grouped and labeled experiences were then expressed as the core themes of the experiences of the study (Moustakas, 1994). This third step of the modified van Kaam method disclosed five main themes and several important experiences. These findings were all critical in addressing the central research question and five subquestions of the study.

Final identification of themes. This fourth step of the modified van Kaam method required the examination and review of themes and important experiences alongside the record transcripts of all the 10 participants. This was performed to strengthen the meanings and impact of the five main themes and important experiences discovered. The following questions were suggested by Moustakas (1994):

1. Are they expressed explicitly in the complete transcription?
2. Are they compatible if not explicitly expressed?
3. If they are not explicit or compatible, they are not relevant to the participant's experience and should be deleted. (pp. 120-121)

Individual textural descriptions. The corroborated main themes and important experiences from the previous stages were employed to establish the individual textual descriptions of the 10 participants (Moustakas, 1994). The computer software program NVivo was used to categorize the summarized individual textural descriptions of the participants. Moustakas (1994) related that the individual textural descriptions of the lived experiences of the participants fuse conspicuously both the themes and important experiences to respond to the "what" of the appearing phenomenon (p. 78). For this stage, verbatim examples were again included and the summarized textual

descriptions for each of the 10 participants can be seen in Appendix F.

Individual structural descriptions. The discovered individual structural descriptions reported the important lived experiences of the 10 participants with regard to the current state of online terrorist recruitment in the United States. The individual structural descriptions were modeled from the preceding stage or the individual textural descriptions. The individual structural descriptions can be seen in Appendix B.

Individual composite descriptions. This step merges the individual textural and structural descriptions from the two previous stages discussed. Moustakas (1994) explained this as "an integration of individual structural into a group or universal description" (pp. 180-181). I then completed this by incorporating the formed themes and important experiences.

Consequential descriptions and actual lived experiences from the findings in the previous stages were then created. The data in this stage were gathered from both the individual and structural descriptions and can be seen in Appendix B.

Composite textural-structural descriptions. The last and final step of the modified van Kaam method by Moustakas (1994) was performed by combing the results of the composite textural and composite structural descriptions as discussed in the previous stages of the seven-step method (see Appendix B). Moustakas (1994) stated that the seventh step is where the "composite description of the meanings and essences of the experience" (p. 108) correspond to the group in general or in a universal manner.

Summary

Five main themes answered the five subquestions of the study. Findings indicated that (a) forums with private e-mails are still one of the major recruitment strategies used, but social media networks are quickly catching up (e.g., Facebook, Twitter, Instagram, Tumblr, and YouTube); (b) the role of the United States as a leader of website hosting increases the freedom for groups to take advantage of a greater recruitment reach; (c) current measures are not enough to counter online terrorist recruitment efforts; (d) the direction in which terrorist recruitment is heading is constantly going forward, increasing, and progressing through the use of the Internet; and (e) online terrorist recruitment continues to evolve and develop by reaching greater audiences through different social media and networking sites.

The central research question was answered based on the findings from the five subquestions. In regards to how the use of the Internet by terrorists has shaped international terrorism, a the main finding was that terrorists no longer have to depend on traveling to far distances or doing face-to-face meetings in order to recruit or plan terrorist attacks. Instead, free and inexpensive Internet programs, as well as advanced encryption software, have allowed terrorists to operate from anywhere in the world. However, although the Internet has been a good method for recruitment, face-to-face communication is also considered effective. Even though the United States government and other international measures have maximized efforts in monitoring suspicious individuals and websites online, major counterterrorism challenges in shutting down terrorist websites are still present. Therefore, additional counterterrorism strategies are needed as online terrorist recruitment continues to evolve and develop by reaching greater audiences through different social media and networking sites.

Analysis of the Findings

This study was designed to answer one central research question, which was how the use of the Internet by terrorists has shaped international terrorism, and five

subquestions, which were the Internet strategies of recruitment used by terrorist organizations, ways in which terrorist Internet recruitment efforts were supported by the United States, measures in place to counter online terrorist recruitment efforts, direction in which terrorist recruitment is heading, and how online terrorist recruitment is evolving in the 21st century.

Interpretation of the Findings

The central research question of this study was this: How has the use of the Internet by terrorists shaped international terrorism? Based on the findings from the five subquestions, the use of the Internet by terrorists has shaped international terrorism in that it has resulted in major challenges for counterterrorism agencies in the United States and abroad due to the ability of terrorists to easily close, change, and create new websites or accounts. In addition, counterterrorism experts also have to deal with advanced encryption software and the anonymity of terrorist suspects. Terrorists no longer have to depend on traveling to far distances or doing face-to-face meetings in order to recruit or plan terrorist attacks. Instead, free and inexpensive Internet programs, as well as advanced encryption software, have allowed terrorists to operate from anywhere in the world. Therefore, through the use of the Internet, terrorists are able to attract other like-minded individuals or sympathizers to their cause. Although the Internet has been a good method for recruitment, face-to-face communication is also considered effective.

In addition, the Internet has increased terrorist organizations' abilities to recruit potential members through forums with private e-mails and social media networks such as Facebook, Twitter, Instagram, Tumblr, and YouTube. The Internet is used by terrorist organizations to distribute training and informational materials such as manuals, handbooks, and pamphlets with web links to instructional videos and audios. The role of the United States as a leader of website hosting increases the freedom for terrorist groups to take advantage of a greater recruitment reach. Even though United States government agencies, such as the FBI, and other international measures, such as the EU Counter-Terrorism Action, have maximized efforts in monitoring suspicious individuals and websites online, major counterterrorism challenges in shutting down terrorist websites are still present. Therefore, additional counterterrorism strategies are needed as online terrorist recruitment continues to evolve and develop by reaching greater audiences through different social media and networking sites.

Furthermore, the Internet has allowed terrorist organizations to move away from organized group attacks and focus on lone wolf terrorist attacks carried out by recruits that take place all over the world. As a result, the Internet has made terrorist attacks less challenging to carry out due to online tools that allow terrorists to spread their message through social media, video and voice communication programs, terrorist websites, e-mail accounts, and online magazines. Counterterrorism actions, such as drone strikes by the United States, are used as part of terrorists' propaganda to recruit sympathizers. Different countries, such as Saudi Arabia, Jordan, Indonesia, and Singapore, have taken steps to counter terrorism through means such as de-radicalization; however, the advancement of Internet tools requires continuous improvement in counterterrorism measures from all countries, including the United States.

The findings from the central research question concurred with the logical connection of the asymmetric conflict theory, which guided this study. Stepanova's (2008) asymmetric conflict theory is described as "a conflict in which the resources of two belligerents differ in essence and in the struggle, interact and attempt to exploit each other's characteristic weaknesses" (Princeton

University, 2014, para. 2). Terrorists are asymmetric actors who are looking to take advantage of their opponent's weaknesses, while the stronger actor seeks to take advantage of the terrorist's weaknesses (Hedges, 2007). Therefore, policymakers and practitioners should continue to recognize terrorist tactics and respond to them in a timely and effective manner, which is vital to national security (Hedges, 2007). In addition, a proactive approach to reduce the danger to open society from online threats is paramount (Heickerö, 2008). As Heickerö (2008) reported, a proactive approach includes gaining knowledge and developing strategies and tactics for counteraction. In addition, cooperation between authorities and organizations around the globe is recommended.

Subquestion 1

Subquestion 1 was as follows: What Internet strategies of recruitment are used by terrorist organizations? The results of Subquestion 1 indicated that forums with private e-mails are still one of the major recruitment strategies used, but social media networks are quickly catching up (e.g., Facebook, Twitter, Instagram, Tumblr, and YouTube). The Internet is also used for the distribution of training and informational materials such as manuals, handbooks, and pamphlets with web links to instructional videos and audios. In addition, the Internet and online profiles of individuals are used as recruiting tools to identify and search for potential members.

The theme and important experiences from Subquestion 1 revealed that terrorists are small substate actors who have less power than nation-states that they are fighting against. This therefore forces them to use unorthodox means, such as the Internet, to achieve their goals (Mount Holyoke College, 2014). The role of the Internet in communication and coordination has been instrumental for groups whose global members and affiliates operate under secrecy (Hedges, 2007). Hedges (2007) related that the Internet has truly aided international jihad by making the tactics and experiences of different insurgent and terrorist groups, from those that are inexperienced to the most professional, available to all. Therefore, terrorists from all experience levels have access to tactics that were forged and refined in places such as Samara, Gaza, Kabul, and Humburg. They can then use these tactics to carry out attacks around the world.

In addition, counterterrorism activities by countries such as the United States are negatively portrayed by terrorists with the goal of recruiting sympathizers and inspiring terrorist action (Thomas, 2003). Terrorism may be the most asymmetrical of all forms of political violence (Stepanova, 2008). In this age of information and mass communications, of critical importance is terrorism's destabilizing effect on national, international, human, and public security, as well as its ability to affect politics (Stepanova, 2008).

Subquestion 2

Subquestion 2 was as follows: In what ways are terrorist Internet recruitment efforts supported by the United States? The results of Subquestion 2 indicated that the role of the United States as a leader of website hosting increases the freedom for groups to take advantage of a greater recruitment reach. In addition, even if the United States Government is maximizing their efforts in monitoring suspicious individuals and websites online, this still could not fully translate into shutting down these websites. The United States Government also does not condone or support any Internet recruitment efforts by terrorist groups.

Individuals in the United States use the Internet to discuss their fundamental human rights. The terrorists are aware of this issue and are exploiting citizens by responding to their issues on the Internet (UNODC, 2012). Therefore, the use of the Internet for terrorist purposes creates both challenges

and opportunities in the fight against terrorism (UNODC, 2012).

Subquestion 3

Subquestion 3 was the following: What measures are in place to counter online terrorist recruitment efforts? The results of Subquestion 3 indicated that that current measures are not enough to counter online terrorist recruitment efforts. However, some measures are done by monitoring and identifying suspicious individuals and groups by the FBI to stop terrorists from further recruiting. In addition, some measures at the national and international levels have been created to closely monitor Internet related terrorism actions.

The theme and important experiences for Subquestion 3 are in line with the UNODC's (2012) report that terrorists' use of the Internet also provides counterterrorism agencies, such as the Center for Strategic Counterterrorism Communications, with the ability to gather intelligence and other activities to prevent and counter acts of terrorism, and gather evidence for prosecution. Terrorist websites, chat rooms, and other Internet communications provide counterterrorism agents with a great amount of knowledge on terrorist functioning, activities, and targets. Electronic data may be compiled and analyzed by counterterrorism agents. In addition, more advanced tools are developed by law enforcement, intelligence, and other authorities to prevent, detect, and deter terrorist activities. Dedicated translation resources are also expanding in order to identify possible terrorist threats. However, additional counterterrorism measures are still needed as there is currently no universal instrument that specifically addresses terrorist Internet threat. Therefore, with the increasing use of the Internet for terrorist purposes, a proactive and coordinated response by member states is needed.

Subquestion 4

Subquestion 4 was this: In what direction is terrorist recruitment heading? The results of Subquestion 4 indicated that the direction in which terrorist recruitment is heading is constantly
going forward, increasing, and progressing through the use of the Internet. The direction will not fully be progressive as skills and proficiency cannot be fully transferred through the Internet.
The theme and important experience from Subquestion 4 revealed that terrorists will continue to be creative with inciting acts of terrorism through the use of the Internet because of its advantages, such as reducing the likelihood of detection and obscure their identity (UNODC, 2012). Therefore, even though face-to-face recruitment and meetings are still used, terrorists are aware of the benefits of Internet technology and therefore will continue to exploit its use for the purposes of terrorism (UNODC, 2012).

Subquestion 5

Subquestion 5 was as follows: How is online terrorist recruitment evolving in the 21st century? The results of Subquestion 5 indicated that online terrorist recruitment continues to evolve and develop by reaching greater audiences through different social media and networking sites. In the 21st century, online terrorist recruitment continues to evolve by transferring terrorists' knowledge and skills in a timely and more convenient way through the Internet. However, face-to-face encounters and communication are still more effective.

The theme and important experiences from Subquestion 5 revealed that although face-to-face encounters and communication are more effective, current recruitment focuses on using the latest Internet technology such as Skype, Twitter, Vine video apps, training videos, video games, YouTube videos, e-mails, and online magazines. These tools assist terrorist organizations with avoiding counterterrorism measures. Therefore,

unlike nation-states, terrorists have the option to remain completely anonymous until they commit an act of terror (Mount Holyoke College, 2014). Through the use of the Internet, they have developed skills in operating from remote locations, avoiding detection by law enforcement surveillance, and evading designated security checkpoints (Theohary & Rollins, 2011). Hence, terrorists use their differences to compensate for their disadvantages against nation-states (Mount Holyoke College, 2014).

Conclusion

The study bridged the gap in knowledge by exploring, understanding, and explaining the perceptions of 10 American terrorist experts on how the use of the Internet by terrorists has shaped international terrorism. Findings for the central research question indicated that terrorists no longer have to depend on traveling to far distances or doing face-to-face meetings in order to recruit or plan terrorist attacks. Instead, free and inexpensive Internet programs, as well as advanced encryption software, have allowed terrorists to operate from anywhere in the world. However, although the Internet has been a good method for recruitment, face-to-face communication is also considered effective. Even though the United States government and other international measures have maximized efforts in monitoring suspicious individuals and websites online, major counterterrorism challenges in shutting down terrorist websites are still present. Therefore, additional counterterrorism strategies are needed as online terrorist recruitment continues to evolve and develop by reaching greater audiences through different social media and networking sites.

As policymakers and practitioners, counterterrorism agencies and organizations should not ignore the limitations of the Internet, but should recognize the opponents' tactics and respond to them in a timely and effective manner. By being proactive about international terrorism and by learning to track communication that is being transmitted on the Internet, the United States could respond to this crisis immediately and effectively.

When US government agencies are proactive in countering terrorist intelligence, then the citizens could be rest assured that international terrorism is not going to be a threat in our country. A proactive approach to learning about international terrorism is imperative to the national security of the United States and other countries, thus saving the lives of the American people and first responders and adding to the effort to make continuous improvements in the nation's homeland security.

References

1. A&E Television Networks. (2014). *The invention of the Internet*. Retrieved from http://www.history.com/topics/inventions/invention-of-the-internet

2. Berg, B. (2009). *Qualitative research methods for social sciences* (7th ed.). Boston, MA: Pearson.

3. Bogdanoski, M., & Petreski. D. (2013). Cyber terrorsim-global security threat. *Contemporary Macedonian Defense – International Scientific Defence, Security and Peace Journal*, *13*, 59-72. doi.327.88:004.738.5-027.22

4. British Broadcasting Cooperation News (2009, January 4). *Who are Hamas?* Retrieved from http://news.bbc.co.uk/2/hi/1654510.stm

5. Brown, I., & Korff, D. (2009). Terrorism and the proportionality of Internet surveillance. *European Journal of Criminology*, *6*, 119-134. doi:10.1177/1477370808100541

6. Caldwell, I. (2008). Terror on YouTube: The Internet's most popular sites are becoming tools for terrorist recruitment. *The Forensic Examiner*, *17*(3). Retrieved from http://www.theforensicexaminer.com/

7. Conway, M. (2007). *Terrorism and Internet governance: Core issues*. *Disarmament Forum*, *2007*(3), 23-24. Retrieved from http://www.unidir.org/publications/disarmament-forum

8. Creswell, J. W. (2010). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage Publication.

9. Denning, D. (2009). Terror's web: How the Internet is transforming terrorism. In Y. Jewkes & M. Yar (Eds.), *Handbook on Internet crime* (pp. 194-213). New York, NY: Routledge.

10. Federal Bureau of Investigations. (2005). *Terrorism 2002-2005*. Retrieved from http://www.fbi.gov/stats-services/publications/terrorism-2002-2005/

11. Federal Emergency Management Agency. (2013). *4: Terrorism*. Retrieved from http://www.fema.gov/media-library-data/20130726-1549-20490-0802/terrorism.pdf

12. Forest, J. (2006). *Teaching terror: Strategic and tactical learning in the terrorist world*. New York, NY: Rowman and Littlefield.

13. Freiburger, T., & Crane, J. S. (2008). A systematic examination of terrorist use of the Internet. *International Journal of Cyber Criminology*, *2*(1), 309-319. Retrieved from http://www.cybercrimejournal.com/tinacraneijccjan2008.htm

14. Gaibulloev, K., & Sandler, T. (2013). Symposium advances in the study of economics of terrorism: Determinants of the demise of terrorist organizations. *Southern Economic Journal*, *79*, 774-792. doi 10.4284/0038-2012.269

15. George Mason University History News Network. (2014). *When was the Internet invented?* Retrieved from http://hnn.us/article/142824

16. Gohel, S. M. (2009). *The Internet and its role in terrorist recruitment and operational planning*. Retrieved from www.ctc.usma.edu/posts/the-Internet-and-its-role-in-terrorist-recruitment-and-operational-planning

17. Gray, D., & Head, A. (2009). The importance of the Internet to the post-modern terrorist and its role as a form of safe haven. *European Journal of Scientific Research, 25*(3), 396-404. Retrieved from http://www.europeanjournalofscientificresearch.com/

18. Gul, I. (2010). Transnational Islamic networks. *International Review of the Red Cross, 92*, 1-25. doi:10.1017/S181638311000129

19. Hardouin, P., & Weichhardt, R. (2006). Terrorist fund raising through criminal activities.
20. *Journal of Money Laundering Control*, *9*, 303-308. doi:10.1108/13685200610681823

21. Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report*, *17*(2), 510-517. Retrieved from http://www.nova.edu/ssss/QR/QR17-2/harper.pdf

22. Hastings, D. (2014, August 29). ISIS recruits children to perform beheadings, shoot rifles, and carry out terrorist attacks. *New York Daily News*. Retrieved from http://www.nydailynews.com/news/world/isis-training-children-behead-launch-terrorist-attacks-article-1.1921995

23. Hedges, J. W. (2008). Eliminating the learning curve. *Journal of Applied Security Research*, *3*, 71-91. doi:10.1300/J530v03n01_07

24. Hegghammer, T. (2013). The recruiter's dilemma: Signalling and rebel recruitment

tactics. *Journal of Peace Research*, 50, 3-16. doi:10.1177/0022343312452287

25. Heickerö, R. (2008). *Terrorism online and the change of modus operandi*. Retrieved from http://www.unidir.ch/files/conferences/pdfs/information-warfare-and-cyber-terrorism-en-1-69.pdf

26. Hoffman, D. (1996). *The web of hate: Extremists exploit the Internet*. New York, NY: Anti-Defamation League.

27. Homeland Security Institute. (2009). *The Internet as a terrorist tool for recruitment and radicalization of youth*. Retrieved from http://www.homelandsecurity.org/docs/reports/Internet_Radicalization.pdf

28. Hummel, M. (2008). Internet Terrorism. *The Homeland Security Review*, *2*(2), 117-130. Retrieved from http://www.calu.edu/business-community/clpp/publications/the-homeland-security-review/index.htm

29. Hunt, J. (2011). The new frontier of money laundering: How terrorist organizations use cyber laundering to fund their activities, and how government s are trying to stop them. *Information and Communications Technology Law*, *20*, 133-152. doi:10.1060/13600834.2011.578933

30. Internet Corporation for Assigned Names and Numbers. (2014). *Beginner's guide to Internet protocol (IP) address*. Retrieved from https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf

31. Jackson, T. (2007). Internet DIY for terror bombs. Terror on the Internet: The new arena, the new challenges. *Palestine-Israel Journal of Politics, Economics and Culture*, *14*(2), 107-108. Retrieved from http://www.pij.org/

32. Jazib, I. H. (2011). *Terrorist recruit youth online*. Retrieved from http://www.weeklypulse.org/details.aspx?contentID=1433&storylist=9

33. Kaplan, E. (2009). *Terrorists and the Internet*. Retrieved from http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005

34. Kershaw, S. (2004, February 19) Washington guardsman charged with trying to spy for AlQaeda. *New York Times*. Retrieved from www.nytimes.com/2004/02/19/us/washington-guardsman-charged-with-trying-to-spy-for-al-Qa'ida.htmlr

35. LaChow, I., & Richardson, C. (2007). Terrorist use of the Internet: The real story. *Joint Force Quarterly*, *45*, 100-103. Retrieved from http://www.dtic.mil/doctrine/jfq/jfq.htm

36. LeCompte, M. D., & Schensul, J. J. (1999). Analyzing and interpreting ethnographic data. In M. D. LeCompte & J. J. Schensul (Eds.), *Ethnographer's toolkit* (pp. 45-81). Walnut Creek, CA: Sage Publications.

37. Linux Information Project. (2005). *Host definition*. Retrieved from http://www.linfo.org/host.html

38. Lubold, G. (2010). *Internet aids terrorist recruiting, radicalization, Pentagon says*. Retrieved from http://www.csmonitor.com/USA/Military/2010/0310/Internet-aids-terrorist-recruiting-radicalization-Pentagon-says

39. Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research*, *11*(3), 8. Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/1428/3027

40. Michael, G. (2013). The new media and the rise of exhortatory terrorism. *Strategic Studies Quarterly*, *7*(1), 40-68. Retrieved from http://www.au.af.mil/au/ssq/

41. Morse, J. M. (1994). Designing funded qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp.220-235). Thousand Oaks, CA: Sage Publications.

42. Mount Holyoke College. (2014). *Why terrorists use the Internet*. Retrieved from http://www.mtholyoke.edu/~lwpoole/politics116/why.html

43. Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications.

44. Networking and Information Technology Research and Development Program. (2014). *Definition of "Internet"*. Retrieved from http://www.nitrd.gov/fnc/Internet_res.aspx

45. Office of Intelligence and Analysis. (2009). *Reference aid: U//FOUO domestic extremism lexicon*. Retrieved from http://www.fas.org/irp/eprint/lexicon.pdf

46. Princeton University. (2014). *Asymmetric warfare*. Retrieved from https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Asymmetric_warfare.html

47. Radlauer, D. (2013). *Virtual communities as pathways to extremism*. Retrieved from http://www.asymmetricconflict.org/articles/virtual-communities-as-pathways-to-extremism/

48. Richards, L., & Morse, J. (2007). *Readme first for a user's guide to qualitative methods* (2nd ed.). Thousand Oaks, CA: Sage Publications.

49. Roberts, B. (2000). *Asymmetric conflict 2010*. Retrieved from http://www.wslfweb.org/docs/dtraasco/asymmetric.pdf

50. Schmidle, R. (2010). Positioning theory and terrorist networks. *Journal of the Theory of Social Behavior*, *40*, 65-78. doi:10.1111/j.1468-5914.2009.00421.x

51. Shetret, L. (2011). *Use of the Internet for counter-terrorist purposes*. Retrieved from http://www.globalct.org/images/content/pdf/policybriefs/LS_policybrief_119.pdf

52. Singer, N. (2012). U.S. is tightening web privacy rule to shield young. *New York Times.* Retrieved from http://www.nytimes.com/2012/09/28/technology/ftc-moves-to-tighten-online-privacy-protections-for-children.html?_r=0

53. Soriano, M. (2012). The vulnerabilities of online terrorism. *Studies in Conflict and Terrorism*, *35*, 263-277. doi:10.1080/1057610X.2012.656345

54. Soriano, M. (2013). The dynamics of the creation, evolution, and disappearance for terrorist Internet forums. *Internal Journal of Crime and Violence*, *7*(1).64-178. Retrieved from http://www.ijcv.org/index.php/ijcv

55. Stepanova, E. (2008). *Terrorism in asymmetrical conflict: Ideological and structural aspects*. New York, NY: Oxford University Press.

56. The White House. (2011). *National strategy for counterterrorism*. Retrieved from http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf

57. Theohary, C., & Rollins, J. (2011). *Terrorist use of the Internet: Information operations in cyberspace*. Retrieved from http://www.fas.org/sgp/crs/terror/R41674.pdf

58. Thomas, T. L. (2003). Al Qaeda and the Internet: The danger of "cyberplanning". *United States Army War College Quarterly*, *33*(1), 112-113. Retrieved from http://www.carlisle.army.mil/usawc/parameters/Articles/03spring/thomas.pdf

59. Thomas, T. S., & Casebeer, W. D. (2004). *Violent non-state actors: Countering dynamic systems*. Retrieved from http://www.au.af.mil/au/awc/awcgate/nps/casebeer_mar04.pdf

60. Towson University. (2014). *What is a nation-state?* Retrieved from http://www.towson.edu/polsci/ppp/sp97/realism/whatisns.html

61. Tsfati, Y., & Weimann, G. (2002). www.terrorism.com: Terror on the Internet. *Studies in Conflict and Terrorism*, *25*, 317-332. doi:10.1080/10576100290101214

62. Tucker, D. (2008). Terrorism, networks, and strategy: Why the conventional wisdom is wrong. *Homeland Security Affairs*, *4*(2). Retrieved from http://www.hsaj.org/

63. U.S. Department of Homeland Security. (2009). *Office of intelligence and analysis reference aid: U//FOUO domestic extremism lexicon.* Retrieved from http://www.fas.org/irp/eprint/lexicon.pdf

64. U.S. Department of State. (2014). *Center for strategic counterterrorism communications*. Retrieved from http://www.state.gov/r/cscc/

65. United Nations Interregional Crime and Justice Research Institute. (2014). *Terrorism and the Internet*. Retrieved from http://www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/terrorism/

66. United Nations Office of Drug and Crime. (2012). *The use of the Internet for terrorist purposes*. Retrieved from
67. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

68. United Nations. (2014). *About UN membership*. Retrieved from http://www.un.org/en/members/about.shtml

69. University of California, Davis. (2014). *Types of samples*. Retrieved from http://psychology.ucdavis.edu/faculty_sites/sommerb/sommerdemo/sampling/types.htm

70. University of South Alabama. (2013). *Chapter 12: Qualitative research*. Retrieved from http://www.southalabama.edu/coe/bset/johnson/lectures/lec12.htm

71. Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*. Washington, DC: United States Institute of Peace Press.

72. Weimann, G. (2007). Using the Internet for terrorist recruitment and mobilization. In B. Ganor, K. Von Knop, & C. Duarte (Eds.), *Hypermedia seduction for terrorist recruiting* (pp. 47-58). Washington, DC: IOS Press.

73. Weimann, G. (2010). Terror on facebook, twitter, and youtube. *Brown Journal of World Affairs*, *16*(2), 45-54. Retrieved from http://www.bjwa.org/

74. Weimann, G. (2013) *Planning terrorist actions with media as a major consideration*. Retrieved from http://thephilanews.com/planning-terrorist-actions-with-the-media-as-a-major-consideration-39834.htm

75. Weimann, G., & Von Knop, K. (2008). Applying the notion of countering online terrorism. *Studies in Conflict and Terrorism*, *31*, 883-902. doi:10.1080/10576100802342601

76. Wiener, G. (2010). *The Internet.* Farmington Hills, MI: Greenhaven Press