



NETworked Radicalization: *A Counter-Strategy*

A Special Report by

The George Washington University
Homeland Security Policy Institute

The University of Virginia
Critical Incident Analysis Group

THE GEORGE WASHINGTON UNIVERSITY

HOMELAND SECURITY
POLICY INSTITUTE

 **CIAG**
Critical Incident Analysis Group

**Homeland Security Policy Institute (HSPI) and
Critical Incident Analysis Group (CIAG)
Task Force on Internet-Facilitated Radicalization***

CO-CHAIRMEN

Frank Cilluffo
Director, HSPI

Gregory Saathoff
Executive Director, CIAG

TASK FORCE MEMBERS

Lord John Alderdice
House of Lords

Abdullah Ansary
Independent Scholar

Eileen Barker
*Professor Emeritus of Sociology with Special
Reference to the Study of Religion
London School of Economics*

Robert Blitzer
*Vice President
ICF International*

Sharon Caudle
*Assistant Director,
Homeland Security
U.S. Government Accountability Office*

John Cohen
*Independent Consultant,
Office of the Program Manager for the ISE,
Office of the Director of National Intelligence*

Guy Copeland
*Vice President
Information Infrastructure Advisory Programs
Computer Sciences Corporation*

Robert Davi
*Actor-Director
National Spokesperson
i-SAFE*

Tal Elharrar
*Policy Analyst,
Counter Terrorism Policy and Coordination
Division
National Security Policy Directorate
Public Safety Canada*

Anna Gray
*Director General
Intelligence Requirements and Strategic
Integration
Royal Canadian Mounted Police
National Security Investigations*

Steve Herrick
*Director of External Relations
American Academy of Religion*

David Heyman
*Director
Homeland Security Program
Center for Strategic and International Studies*

J. Michael Hickey
*Vice President, Government Affairs,
National Security Policy
Verizon*

Mark Juergensmeyer
*Director
Orfalea Center for Global & International
Studies
University of California, Santa Barbara*

Anita Jones
*Professor of Computer Science,
University of Virginia*

Stephen King
*Counsel,
Hunton & Williams*

Mary McCarthy
*Former Senior Director
National Security Council*

Michael McDonell
*Assistant Commissioner
National Security Investigations
Royal Canadian Mounted Police*

Paul Nicholas
*Senior Security Strategist
Microsoft*

Reuven Paz
*Director
Project for the Research of Islamist Movements
(PRISM)*

Dennis Pluchinsky
*Former U.S. State Department Intelligence
Analyst*

Michael Ricciuti
*Partner
Kirkpatrick & Lockhart Preston Gates Ellis LLP*

Julie Ryan
*Assistant Professor
Engineering Management and Systems
Engineering
The George Washington University*

Marc Sageman
Sageman Consulting, LLP

Seth Stodder
*Senior Counsel
Akin Gump Strauss Hauer & Feld, LLP*

Stephen Ulph
*Senior Fellow
The Jamestown Foundation*

Amit Yoran
*Chief Executive Officer
NetWitness Corp.*

* The affiliations of the individual task force members are provided for identification purposes only and do not represent endorsements by those organizations or agencies.

CO-AUTHORS

Frank Cilluffo
Director, HSPI

Gregory Saathoff
Executive Director, CIAG

Jan Lane
Deputy Director, HSPI

Sharon Cardash
Associate Director, HSPI

Andrew Whitehead
Policy Analyst, HSPI

TASK FORCE COORDINATOR

Josh Magarik
Policy Analyst, HSPI

About The Homeland Security Policy Institute

The George Washington University Homeland Security Policy Institute (HSPI) is a nonpartisan “think and do tank” that builds bridges between theory and practice to advance homeland security through a multi and interdisciplinary approach. By convening policymakers and practitioners at all levels of government, academia, and the private sector, HSPI creates innovative strategies and solutions to current and future threats to the nation.

About The Critical Incident Analysis Group

The University of Virginia’s School of Medicine’s Critical Incident Analysis Group (CIAG) is an international interdisciplinary “think-net” from academe, government and business who work to analyze and understand the impact of "critical incidents" on people, communities and social structures. CIAG brings together physicians, social scientists, law enforcement specialists, policy makers, diplomats, military leaders, journalists—and a host of others who are concerned about the profound impact of critical incidents. CIAG is thus an inter-disciplinary applied research and advisory body that combines complementary experience and expertise to understand and to serve.

For further information, please contact:

Homeland Security Policy Institute
The George Washington University
2300 I Street NW, Suite 721
Washington, DC 20037
Phone: 202-994-2437
hspi@gwu.edu
www.homelandsecurity.gwu.edu

The Critical Incident Analysis Group
(CIAG)
UVa School of Medicine
PO Box 800657
Charlottesville, VA 22908-0657
(434) 243-9458
ciag@virginia.edu
www.healthsystem.virginia.edu/internet/ciag

Introduction

Savvy use of the Internet has empowered terror networks to expand their reach beyond national borders by enabling wide distribution of a compelling message and social connectivity with new audiences. Use of computer-mediated communication (CMC) has made a range of terrorist operational activities cheaper, faster, and more secure, including communications, fundraising, planning and coordination, training, information gathering and data mining, propaganda and misinformation dissemination, and radicalization and recruitment. The list is long, and not even complete. Before the Internet, terrorists seeking to communicate with one another through electronic means used telephones or radios, which could be tapped. Terrorists seeking to offer training meant congregating trainers and trainees in a fixed training location, exposing the group to capture or worse. Terrorists or their supporters engaged in fundraising or recruitment often pursued these aims in public settings. And terrorists researching a potential target often did so at public libraries and bookstores, subjecting them to surveillance in these public spaces. Now, with the Internet, all of these same activities can be conducted in relative anonymity from safe locations across the globe:

- Terrorists can draft an email message and save it as a draft rather than sending it, so that anyone with access to that email account can log in and read the message. Known as “dead drops,” these communications are less subject to interception.¹
- Terrorists can post training manuals online or even hack into a legitimate website and hide training materials “deep in seemingly innocuous subdirectories of the legitimate site,” a process known as “parasiting.”²
- Terrorists can conduct research on potential targets online, where both text and imagery, including satellite photography, is frequently available. Google Earth, for instance, has been used to target British soldiers in Iraq with increasing accuracy.³
- Terrorists can appeal anonymously for donations of financial or other support via websites.

Planning and preparations for the 9/11 attacks were facilitated by the Internet. Operatives engaged in the attack used it to communicate. Flight schools were researched through it, as were targets. Its uses have evolved over time and to increasingly gruesome creative effect – witness the videotaped beheadings of Nicholas Berg and Daniel Pearl circulated online to the four corners of the earth. These uses of the Internet, horrific as they may be, are fundamentally static – one way communication directed at a global audience.

¹ See Appendix A. All information provided, without a pinpoint source, originates from task force briefings with subject matter experts and officials with personal experience in dealing with the issues under study. The task force received many briefings of a sensitive nature and some briefers wish to remain anonymous.

² “Examining the Cyber Capabilities of Islamic Terrorist Groups,” Institute for Security Technology Studies at Dartmouth College, November 2003, http://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf.

³ Thomas Harding, “Terrorists 'use Google maps to hit UK troops',” *Telegraph* Online, January 13, 2007, <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/13/wgoogle13.xml>.

What renders the Internet a particularly potent tool is its capacity to foster interaction. Virtual chat rooms make real time, two-way dialogue possible, permitting extremist ideas to be shared, take root, be reaffirmed and spread exponentially. For the post-Iraq (post-2003) generation especially, Internet chat rooms are now supplementing and replacing mosques, community centers and coffee shops as venues for recruitment. In short, cyberspace is now the battlefield, and the “war” is one of ideas. Our adversaries currently have firm possession of that battlefield because they understand this shift and have crafted and disseminated a narrative that resonates and that has served both to energize and expand their ranks. They have woven an effective tale of an imaginary “clash of civilizations” in which, supposedly, a monolithic West has been engaged in an aggressive struggle against a monolithic Islam for centuries, since the time of the Crusades. The messaging is meant to resonate with a younger generation, and reinterpret Islam to suit the agenda of the global extremist “jihadi” Salafist movement.

By its very nature, the Internet “enables groups and relationships to form that otherwise would not be able to, thereby increasing and enhancing social connectivity.”⁴ As a new means of social interaction, it brings together people – friends, family members, or complete strangers – with similar interests and values, and fosters a sense of affiliation and identity. The “killer application” of the Internet is not so much its use as a broadcast tool, but its function as a communications channel that links people in cyberspace, who then meet and can take action in the physical world.⁵

And who are those individuals who will be receptive – or vulnerable – to an extremist message and “call to action” at that nexus where the cyber and physical realms meet? There is no one-size-fits-all explanation, and much still remains to be learned on this count. However, from Toronto to London, from Madrid to Morocco, and in Holland, America and beyond, we have witnessed the effects of radicalization. Some have termed these instances as the rise of “homegrown” terrorism, but the label is something of a misnomer. The Internet has created a largely borderless world and those who participate in terrorist acts are therefore perhaps best understood within this global context, rather than merely a national one.

Preliminary Matters of Scope and Definition

This report focuses on radicalization in the context of the transnational insurgency that is the global extremist “jihadi” Salafist movement. Further, the report explores the relatively delimited question of how to respond to and counter Internet-facilitated radicalization. It does not address wider policy questions, not because they are unimportant, but because they fall outside the scope of this particular study. Key terms are defined as follows:

⁴ John A. Bargh and Katelyn McKenna, “The Internet and Social Life,” *Annual Review of Psychology*, 55, 573-590 (2001), p.2, http://pantheon.yale.edu/~jab257/internet_and_social_life.pdf.

⁵ Ibid, p. 3, citing J. Kang, “Cyber-race,” *Harvard Law Review* 113 (2000): 1150.

- Radicalization is “the process of adopting an extremist belief system, including the willingness to use, support, or facilitate violence, as a method to effect societal change.”⁶
- Recruitment is “the solicitation of individuals to commit terrorist acts or engage in behavior for a terrorism purpose.”⁷
- The global extremist “jihadi” Salafist movement is a transnational insurgency, perhaps best exemplified by al Qaeda but including other groups ascribing to the same ideology. The movement seeks to seize control of the countries of the Muslim world and unite them in a single state (*caliphate*) governed by the extremists’ literal interpretation of Islamic law. The terms “jihad” and “jihadi” appear in quotation marks because extremists have hijacked the concept of jihad, using it – wrongly – to justify acts of violence. Unfortunately, the media and government entities have adopted this incorrect usage, and it has now become part of common parlance. In its true sense, however, jihad refers either to inner struggle (striving for righteous deeds), or to external struggle against aggression and injustice in which strict rules of engagement concerning the protection of innocents apply.⁸

Radicalization is not unique to Islam nor is it a new phenomenon. Historically, extremist beliefs have been used to subvert the ideals of every major religion in the world and Islam is only one of several that terrorists may invoke to justify acts of violence (though such acts run counter to the very tenets of Islam). Indeed, terrorist organizations of all stripes, adhering to any number of extremist belief systems, are present on the Internet and have used it to radicalize and recruit others.

Virtual Propaganda and Radicalization:

Connecting the Dots in the Real World

Propaganda and radicalization matter, whether online, offline or a mixture of the two. Propaganda fuels the radicalization process, and evidence of the effects of that process is disturbing:

Adam Gadahn. An American citizen from California, Gadahn now serves as al Qaeda’s English-language spokesman under the name Azzam al Amriki. He has produced propaganda videos, circulated over the Internet, which extol Muslims to join the global

⁶ Charles E. Allen, “The Threat of Islamic Radicalization to the Homeland,” testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, delivered on March 14, 2007, p. 4.

⁷ Frank Cilluffo, Gregory Saathoff, et al., *Out of the Shadows: Getting Ahead of Prisoner Radicalization*, Special report by The George Washington University’s Homeland Security Policy Institute and the University of Virginia’s Critical Incident Analysis Group, September 19, 2006, p. 3.

⁸ See Appendix A.

extremist “jihadi” Salafist movement and take part in “slitting the throats of the infidel.”⁹ Adept at building networks offline, he was able to carry that ability – along with a sense of moral outrage – to the online environment.

Hassan Abujihaad. Formerly known as Paul R. Hall. “[A]n American-born Muslim convert,” Abujihaad was arrested in March and charged with disclosing secret information about the location of Navy ships to terrorist groups. Abujihaad was in contact with extremists online and had ordered from them videos “that promoted violent jihad.”¹⁰

Christopher Paul. In April 2007, Paul, an American from Ohio, was charged with providing training to al Qaeda operatives, and planning terrorist attacks overseas. He is alleged to have trained with al Qaeda operatives in Pakistan and Afghanistan, and recruited for al Qaeda in Germany. He is also believed to have provided equipment and money to terrorists plotting attacks overseas.¹¹ It is further alleged that Paul watched propaganda videos showing violence against Muslims.¹²

The Madrid Bombings. On March 11, 2004, terrorists detonated a series of explosives placed on Madrid’s commuter trains, killing one hundred ninety-one people. The terrorists are believed to be members of an autonomous network active in North Africa, connected to al Qaeda only by ideology and drawing no more than inspiration from other terrorist groups. The Internet is known to have played a role in promoting extremist ideology among the group. Specifically, among propaganda circulated by the Global Islamic Media Front (GIMF) was speculation as to the impact of an attack prior to Spanish elections.¹³

The London Bombings. On July 7, 2005, four suicide bombers killed themselves and fifty-two others in a series of coordinated attacks on London’s public transportation system, targeting crowded commuter trains and a bus. Three of the bombers were born and raised in Britain. There is no indication that the attacks were planned or supported by al Qaeda or other foreign extremist groups.¹⁴ Instead, the group appears to have formed, planned, and acted on its own.

The Toronto Case. In June 2006, Canadian authorities arrested seventeen people (later eighteen) suspected of plotting a series of terrorist attacks including truck bombings against the Toronto Stock Exchange, a strike on Parliament, the murder of Prime Minister Stephen Harper, and other acts of mass murder. The group appears to have sprung up on its own, its

⁹ Raffi Khatchadourian, “Azzam the American: The Making of an Al Qaeda Homegrown,” *The New Yorker*, January 22, 2007, http://www.newyorker.com/fact/content/articles/070122fa_fact_khatchadourian.

¹⁰ “Judge Orders Terror Suspect Held without Bond” *International Herald Tribune*, March, 23 2007, <http://www.iht.com/articles/ap/2007/03/23/america/NA-GEN-US-Navy-Terror.php>.

¹¹ Peter Selvin, “Jury Indicts Ohio Man for Conspiring With Al-Qaeda,” *The Washington Post*, April 13, 2007, p. A09, <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/12/AR2007041200689.html>.

¹² Kevin Bohn, “Ohio Man Charged With Helping al Qaeda,” *CNN*, April 12, 2007, <http://www.cnn.com/2007/LAW/04/12/terrorism.charges/index.html>.

¹³ Geoff Pingree and Lisa Abend, “Judge Assesses Madrid Attacks,” *The Christian Science Monitor*, April 13, 2006, <http://www.csmonitor.com/2006/0413/p06s02-woeu.html>.

¹⁴ “Report of the Official Account of the Bombings in London on 7th July 2005,” United Kingdom House of Commons, May 11, 2006, p. 21, http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/11_05_06_narrative.pdf.

members radicalized in part by extremist “jihadist” videos downloaded from the Internet and viewed as a part of training exercises.¹⁵

Radicals in the Netherlands. These include the Hofstad Group, which plotted to conduct suicide bombings and assassinate Dutch politicians. One operation allegedly considered was an assault on a nuclear power plant. The Group included immigrants, the descendants of immigrants to the Netherlands, and indigenous Dutch converts to extremist “jihadi” Salafist beliefs; one person who helped provide safe houses to the Group was a former policewoman. Dutch police have identified several examples of Dutch Muslims, mostly young and not religiously trained, who have adopted extremist “jihadi” Salafist beliefs to which they were exposed over the Internet.”¹⁶

Casablanca. In March 2007, a Moroccan man was killed in Casablanca when the explosives he had strapped to his body exploded inside an Internet café. The man and his companions often visited the café to view “jihadist” websites. It appears that the bomb detonated during a struggle with the café’s owner, who wanted to stop the men from downloading and viewing propaganda materials in his shop.¹⁷

The pace of “transformation” is striking and has been accelerating.¹⁸ London police chief Ian Blair has said that the suspects in the plot to bomb airliners in the United Kingdom during the summer of 2006 went “from what would appear to be ordinary lives in a matter of some weeks and months, not years, to a position where they were allegedly prepared to commit suicide and murder thousands of people.”¹⁹ This toxic combination of speed and potential consequences brings into stark relief the urgent need to better understand how and why radicalization occurs, either in person or via the Internet or chat rooms, so that it may be countered.

Online Propaganda and Virtual Radicalization:

The Medium, the Message and Reasons for its Appeal

The Internet facilitates radicalization because it is without peer as a tool for both active and passive communication and outreach. Online chat rooms are interactive venues where aberrant attitudes and beliefs may be exchanged, reinforced, hardened and validated (at least

¹⁵ See Appendix A.

¹⁶ S.J. van Hulst, “Violent Jihad in the Netherlands: Current Trends in the Islamist Terrorist Threat,” Netherlands Ministry of the Interior and Kingdom Relations, 2006, p. 47.

¹⁷ Craig S. Smith, “Companion of Suicide Bomber Questioned over Casablanca Internet Café Blast,” *International Herald Tribune*, March 12, 2007, <http://www.iht.com/articles/2007/03/12/news/morocco.php>.

¹⁸ Stewart Bell, “Jihadization of Youth a ‘Rapid Process,’” *The National Post*, January 26, 2007, <http://www.canada.com/nationalpost/news/story.html?id=25e76872-b309-47a7-841b-938bdd9ffd71&k=76582>.

¹⁹ Michael Holden, “Bomb Suspects ‘Radicalized in Weeks,’” *Reuters*, January 24, 2007, http://today.reuters.co.uk/news/articlenews.aspx?type=topNews&storyID=2007-01-24T175436Z_01_L24334309_RTRUKOC_0_UK-BRITAIN-SECURITY.xml.

in the minds of participants). This mutual affirmation in turn gives rise to a sense of community and belonging – a virtual *ummah* (worldwide Muslim community). Even those who simply lurk in these forums may be at risk, although they may not realize it. As extremist viewpoints are continuously reaffirmed by the like-minded, the doubts of observers/listeners may be assaulted and eroded. CMC has been shown to increase conformity to group norms.²⁰ In studies of racial violence and hate crime over the Internet, it has been demonstrated that the anonymity of the Web and the culture of chat rooms leads to an increased level of endorsement for violence than is actually felt by participants.²¹

As a mechanism to exert influence and mold opinion, the Internet is powerful because it gives voice to potentially everyone and does so in distinctly egalitarian fashion. The case of “*Irhabi* (Terrorist) 007” offers a powerful illustration. Under this pseudonym, and while barely into his twenties, Younis Tsouli rose from obscurity to a position of leadership by participating frequently and enthusiastically in online extremist forums. The sheer volume of Tsouli’s postings began to earn him the trust of other participants and, when he responded positively and energetically to the beheading videos posted on the Web by al Qaeda in Iraq, that group in turn praised and endorsed Tsouli.²²

Indeed, any extremist group, no matter how small, can create a professional-looking website that may reach a wide, geographically dispersed audience of potential recruits. Neo-Nazi groups, for example, “were among the first to seize upon the benefits of cyberspace,”²³ establishing websites, bulletin boards, newsgroups, mailing lists, and chat rooms.²⁴ Just a few years ago, hundreds of websites served terrorists and their supporters.²⁵ Now, ten to twenty-five such sites are thought to generate new material which is mirrored in several thousand others.²⁶

These developments mirror those in society writ large, where use of the Internet is continually expanding and evolving as a means of social networking and mobilization. For example, a number of candidates running for president in 2008 announced their candidacy not at rallies or press conferences, but through videos broadcast on their websites. Almost every top contender is turning to social networking sites, such as MySpace, as “a method of reaching people who are historically not interested in voting.”²⁷ Politicians now maintain blogs, conduct web chats with constituents, and hold virtual town hall meetings to shape public opinion and mobilize popular support.

²⁰ Bargh, *supra* note 4 at p. 8, citing T. Postmes and R. Spears, “Deindividuation and Anti-Normative Behavior: A Meta-Analysis,” *Psychological Bulletin* 123 (1998): 238-259.

²¹ Jack Glaser, Jay Dixit, and Donald P. Green, “Studying Hate Crime with the Internet: What Makes Racists Advocate Racial Violence?” *Journal of Social Issues* 58, no. 1 (2002): 177-193.

²² See Appendix A.

²³ Michael Whine, “Cyberspace – A New Medium for Communication, Command, and Control by Extremists,” *Studies in Conflict and Terrorism* 22 (1999): 233.

²⁴ Phyllis B. Gerstenfeld, et al., “Hate Online: A Content Analysis of Extremist Internet Sites,” *Analysis of Social Issues and Public Policy* 3, no. 1 (2003): 30.

²⁵ Gabriel Weimann, “www.terror.net: How Modern Terrorism Uses the Internet,” United States Institute of Peace, March 2004, p. 2.

²⁶ See Appendix A.

²⁷ Alex Williams, “The Future President, on Your Friends List,” *The New York Times*, March 18, 2007, <http://www.nytimes.com/2007/03/18/fashion/18myspace.html>.

The media posture of the global extremist “jihadi” Salafist movement is, similarly, sophisticated and multidimensional. By way of illustration, al Qaeda has its own official production arm (As-Sahab), for which the GIMF serves as clearinghouse.²⁸ The GIMF itself is a multipronged operation, which to date has used many of the tools of a major public relations effort including television, websites/chat rooms, and word of mouth. Indeed, al Qaeda as we now know it is both an inspirational and operational force. And the movement it has spawned is fuelled by ideology propagated in a range of ways, from simple word of mouth to sophisticated technological means. The Internet facilitates the spread of that ideology and inspiration in various ways, including by serving as a distribution vehicle for videos, songs, videogames and radio broadcasts.²⁹

The primary focus of the movement’s efforts online appears to be youth, including those living in the West. Websites are often flashy and colorful, apparently designed to appeal to “a computer savvy, media-saturated, video game-addicted generation.”³⁰ One site features a game called “Quest for Bush” in which the player fights Americans and proceeds to different levels including “Jihad Growing Up” and “Americans’ Hell.”³¹ These so-called games amount to a dynamic form of propaganda, whose purpose is to transform a generation into radicalized foot soldiers of a global insurgency.³² Videos circulated through websites serve the same purpose, spreading a simple but seemingly compelling message: Islam is under attack and young Muslims have a personal duty to fight in defense of the *ummah*.³³

The images presented in these videos are graphic and calculated to provoke, issue a call to arms and motivate. News footage is included from the Israeli-Palestinian conflict, Iraq, Lebanon, Chechnya, Bosnia, Kosovo, and other “hot spots” around the world. U.S. and allied troops are framed as invaders, occupiers, and destroyers. Civilian casualties of these conflicts, especially Muslim women and children, are depicted as victims of Western aggression, with blood, gore, and tears often emphasized. Exposed to these images over and over again, the viewer may internalize the message, becoming frustrated and enraged over the enormous injustice he perceives to be occurring.³⁴

Once produced only in Arabic, videos are being dubbed, subtitled, or produced in a wider range of languages in order to reach a broader audience.³⁵ Some now include hip-hop and rap musicians whose catchy, melodic messages contain calls to violence. In one such video,

²⁸ Sebastian Usher, “Webcast News Gives Al-Qaeda View,” *BBC News*, September 30, 2005, http://news.bbc.co.uk/1/hi/world/middle_east/4298206.stm.

²⁹ Weimann, *supra* note 25 at p. 4. See also Frank J. Cilluffo, Sharon L. Cardash and Andrew J. Whitehead, “Radicalization: Behind Bars and Beyond Borders,” *Brown Journal of World Affairs* (2007), referencing select concepts/passages in the present report.

³⁰ Bruce Hoffman, “The Use of the Internet by Islamic Extremists,” testimony before the Permanent Select Committee on Intelligence, U.S. House of Representatives, May 4, 2006, p. 5.

³¹ Jose Antonio Vargas, “Way Radical, Dude,” *The Washington Post*, October 9, 2006, p. C01, <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/08/AR2006100800931.html>.

³² See Appendix A.

³³ Hoffman, *supra* note 30 at p. 6. See also Weimann, *supra* note 25 at p. 6.

³⁴ See Appendix A.

³⁵ Frank Gardner, “The Growth of ‘Online Jihadism’,” *BBC News*, October 25, 2006, http://news.bbc.co.uk/2/hi/uk_news/6086042.stm.

titled “Dirty Kuffar [Non-believers],” the rapper “Sheikh Terra” sings with a gun in one hand and a Qur’an in the other; images of Iraqis being killed by American troops are displayed, the terrorist attacks of 9/11 are lauded, and viewers/listeners are called on to fight back.³⁶ Videos were crudely produced, sold for a few cents and in limited distribution before the Internet. Raids of “safe houses” often yield stacks of DVDs, CDs, VHS tapes, and VCDs. The Worldwide Web has made it increasingly easy to produce and circulate these videos globally.³⁷ All of these visuals are accompanied or underpinned, either explicitly or implicitly, by a carefully crafted narrative depicting the Islamic world under siege or attack.

New video-hosting websites like YouTube broaden potential audience reach further. The site receives tens of thousands of new videos daily, and users watch over a hundred million per day, making content difficult to monitor. Though authorities have identified a number of “jihadist” propaganda items on the site – some being viewed by thousands – these are often replaced almost as soon as they are removed.³⁸ Extremists themselves confess the importance of the video as tool. As one said of his radicalization, the “first time I saw an al-Qaeda video, I was ready to go... I wanted to kill the disbelievers.”³⁹

Extremist interpretations of religious doctrine feature prominently on websites, where articles, pamphlets and even libraries of books appear. These texts are devoted to finding justifications, within the context of Islam, for the movement’s violent ideology and acts. This is intended to assure potential recruits, and to reassure those already recruited, of the righteousness of both the cause and the means adopted to further it.⁴⁰ By way of example, consider the following *fatwa* (religious ruling) published online by an Egyptian declaring suicide terrorism to be legitimate within Islam (contrary to the traditional Islamic jurisprudence that it is a violation of the religion and forbidden by God):

He who commits suicide kills himself for his own benefit, while he who commits martyrdom sacrifices himself for the sake of his religion and his nation. While someone who commits suicide has lost hope with himself and with the spirit of Allah, the *Mujahid* [struggler] is full of hope with regard to Allah’s spirit and mercy. He fights his enemy and the enemy of Allah with this new weapon, which destiny has put in the hands of

³⁶ This video was viewed on March 29, 2007 at <http://youtube.com/watch?v=5mcSbUQc3hU>. See also Antony Barnett, “Islamic Rappers’ Message of Terror,” *The Guardian*, February 8, 2004, http://observer.guardian.co.uk/uk_news/story/0,6903,1143499,00.html.

³⁷ See Appendix A.

³⁸ Tariq Panja, “Militant Islamic Groups Turn to YouTube,” *The Washington Post*, February 11, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/02/11/AR2007021100956.html>.

³⁹ Stewart Bell, “Making of a Zealot,” *National Post*, June 30, 2006,

<http://www.canada.com/nationalpost/news/story.html?id=04c78d5f-8003-4d21-b845-d17f47852b71&p=1>.

In online images, “jihadist” leaders are depicted as either heroic or angelic. Fighters are juxtaposed with images of lions, horses, falcons, and other animals to emphasize their bravery, strength, and ferocity. Those who died while fighting are depicted as martyrs for the cause; their images – in life and, sometimes, after death – are juxtaposed with images of flowers, waterfalls, Korans, and beams of light in order to depict the holiness of their sacrifices and the paradise expected to await them after death. See “The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda,” Combating Terrorism Center, U.S. Military Academy, March 2006, <http://www.ctc.usma.edu/CTC%20--%20Islamic%20Imagery%20Project.pdf>.

⁴⁰ See Appendix A.

the weak, so that they would fight against the evil of the strong and arrogant.⁴¹

The virtual world cannot be divorced from the physical realm in which it is grounded, however. It is the complex, iterative and dynamic interplay between the two that helps explain why the extremist narrative resonates and how it spreads. There is no set formula that explains why someone is vulnerable to radicalization, or why a radicalized individual goes on to become a terrorist. As the Department of Homeland Security (DHS)'s Office of Intelligence and Analysis observes, the process of radicalization “varies across ideological and ethno-religious spectrums, different geographic regions, and socioeconomic conditions.”⁴² Social bonds play an important role in the radicalization process. Some argue that they “are the critical element and precede ideological commitment.”⁴³

This is especially true for diaspora communities around the world, which often turn inward to seek mutual support, a sense of identity, and an enhanced sense of dignity. Youth in these communities, including second- and third-generation descendants of immigrants, may feel alienated both from their parents' culture and from the surrounding culture of the country in which these youth live. They may therefore rely on each other to provide a sense of community, making it considerably easier for a single radicalized individual to influence others. Shaming of a group or community is transmitted by first-generation immigrants fleeing economic and social conditions elsewhere to the next generations (second, third and fourth) who may not feel part of either their new land or the land that their parents fled. Their ambivalence about their parents and their new country may lead to disturbance in them as a group and sometimes to violent actions that their individual personal profiles would not immediately have suggested.⁴⁴

While particularly evident in Europe, similar senses of alienation exist within American Muslim communities – although barriers to assimilation are on average much lower in the United States.⁴⁵ American Muslim community leaders have expressed their perception of “the roll back of basic civil liberties in America” since 9/11. Of specific concern is the perception of how the *USA PATRIOT Act* was implemented, and the subsequent “imprison[ment of] well over 1,200 Muslim and Arab men using the pretext of immigration violations.”⁴⁶

⁴¹ Gabriel Weimann, “Virtual Disputes: The Use of the Internet for Terrorist Debates,” *Studies in Conflict and Terrorism* (2006): 634.

⁴² Allen, *supra* note 6 at p. 5.

⁴³ Angela Gendron, “Militant Jihadism: Radicalization, Conversion, Recruitment,” Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University, April 2006, p. 9, <http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-4.pdf>.

⁴⁴ Lord Alderdice, “The Individual, the Group and the Psychology of Terrorism,” *International Review of Psychiatry* (June 2007), in press.

⁴⁵ Cilluffo and Saathoff, *supra* note 7 at pp 9-10.

⁴⁶ Parvez Ahmed, “Terror in the Name of Islam: Unholy War not Jihad” (paper presented at the ‘Sacred Violence: Religion and Terrorism’ conference held by the Institute for Global Security, Law and Policy at the Case Western University School of Law, Cleveland, Ohio, March 30, 2007), citing figures in “The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks,” Office of the Inspector General, U.S. Department of Justice, April 1, 2003.

Terror networks target young men by giving them “interpretations of Koranic verses that have been chosen so as to lead them to rebel against their parents, their families, and even against the society in which they live.”⁴⁷ Veterans of combat – in Iraq and other places – are particularly useful for recruiting youth, who respect the veterans’ anti-authoritarian attitude and “street credibility.” Therefore, there may also be an element of youthful rebellion in all of this, as some may be swept up by the romanticism of joining an “international brigade.”⁴⁸

Through social network analysis, a remarkably complex array of interactions – between terrorists, their supporters, potential recruits and targeted audiences, and many others relevant to understanding this movement – is rendered easier to understand. Social network analysis offers “a way to visualize the nodes in the network and how things move through that network such as weapons, pieces of knowledge or people...”⁴⁹ The Internet, by virtue of being the preferred mode of social connectivity among this generation, coupled with an understanding of social networking can better inform our understanding of the radicalization process and what moves one from sympathizer to activist.

A psychological understanding of radicalization via the Internet includes an appreciation of large and small group psychology.⁵⁰ An important means of understanding large group psychology is through the prism of cultural identity. Historically, geography was a major determinant of cultural, ethnic and religious identity. Whether contained within a country of origin or within ethnic or immigrant communities, spread of these large group identities was only as effective as the limited transportation possibilities at that time. If jet transportation has accelerated the process of large group identity formation, it may be that the Internet is transforming large group identity formation from a lateral, physical process to a metastatic, technological process. Previous boundaries have little relevance. Now, through chat rooms and websites, boundaries are formed and broken instantaneously, so that persons in Seattle, Singapore and Stockholm can meet, establish and maintain ideologic bonds, perhaps even stronger than if they had been forged in face-to-face encounters. Extremist radicalization, whether secular or religious, is inherently a group phenomenon. This can begin in open environments such as universities, or closed environments such as prisons. For large groups, there is a resonance to shared cultural, ethnic and religious symbols. Real events that can be perceived as oppressive or humiliating – described in psychiatric literature as “chosen traumas”⁵¹ – may be memorialized through language, images and music, and may then powerfully resonate within the intended audience and in subsequent generations.

An understanding of small group psychology and sociology is also vital. According to Atran, members of individual cells usually show remarkable in-group homogeneity (age, place of

⁴⁷ Gendron, *supra* note 43 at p. 9.

⁴⁸ See Appendix A.

⁴⁹ Bryan Bender, “Antiterrorism Agency Taps Boston-area Brains,” *The Boston Globe*, March 27, 2007, http://www.boston.com/news/nation/washington/articles/2007/03/28/antiterrorism_agency_taps_boston_area_brains/.

⁵⁰ Emerging neuropsychiatric research is also important to a psychological understanding of this process.

⁵¹ V. Volkan, *Bloodlines* (Farrar, Straus and Giroux, 1997) 48-49.

origin, residence, educational background, socioeconomic status, and so on).⁵² This homogeneity can be established and shaped by extremists through initial and subsequent interactions on the Internet, using aliases as the initial identifying feature and progressing in a give-and-take process.

A Snapshot of Countering Efforts To-Date

To generate a sense of context, a sampling (albeit unscientific) of noteworthy and creative initiatives—many of which are not very well known—are highlighted below. Admittedly, some of these measures may be limited in their ability to counteract the impact of the extremist narrative, which is being accepted and adopted by an important minority around the world. It is also important to recognize that certain countries and institutions may be sending mixed messages by simultaneously engaging or acquiescing in other activities that would seem to undercut the efforts referenced.

Britain.

- An important grassroots effort directed against radicalization in the U.K. is “the Radical Middle Way,” an initiative aimed at articulating a mainstream understanding of Islam that is dynamic and relevant, particularly to young British Muslims. Partially funded by the government, the project is a collaboration among several British Muslim organizations. It seeks to undermine the extremists’ message that violence is a legitimate way of practicing Islam. To this end, the Radical Middle Way maintains a website that features presentations by scholars of religion on the tenets of Islam. The project has also held roundtables with radical groups in Britain, seeking to establish dialogue as a way of encouraging extremists to renounce their radical beliefs.
- Pursuant to a recently announced UK government initiative, Muslim “opinion formers” (imams and others) will be offered “special training in how to face down extremism and be role models for moderation and tolerance.” There is also to be “a major increase in the number of ‘forums against extremism’—regional groups which meet regularly and which were set up in the wake of the July 7 London bombings to enable Muslims to discuss ways of tackling extremism.”⁵³
- In the wake of 9/11, UK intelligence officials posted messages on websites known to be accessed by extremists, to appeal for information about the perpetrators. The requests emphasized that people of all faiths, including Muslims, were murdered that day.⁵⁴

⁵² Scott Atran, “Commentary: A Failure of Imagination (Intelligence, WMDs and ‘Virtual Jihad’),” *Studies in Conflict and Terrorism* 29 (2006): 263-278.

⁵³ Patrick Hennessy, “Muslim Leaders Helped to Tackle Extremists,” *Sunday Telegraph*, February 2, 2007, <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/04/01/nislam01.xml>.

⁵⁴ Maura Conway, “Terrorist ‘Use’ of the Internet and Fighting Back,” (paper prepared for presentation at the “Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities” conference held by the Oxford Internet Institute, Oxford, United Kingdom, September 8-10, 2005), p. 24.

Egypt.

- The Muslim Brotherhood has denounced terrorist attacks committed by “jihadists,” accusing them of having no “conscience or religion.”⁵⁵
- Ali Gomaa, Grand Mufti of Egypt, has issued a statement declaring that “women have equal political rights in Islam,” and that nothing in Islamic principles prevents women from holding high institutional positions including “the highest office in Muslim nations.”⁵⁶ This is a direct challenge to the extremists, who seek to enforce incredibly strict restrictions on women.

Indonesia.

- Kyai Haji Abdurrahman Wahid, the country’s first democratically elected president, now serves as head of a major Muslim congregation and as senior advisor to the LibforAll Foundation; in those capacities he advocates religious tolerance, pluralism and democracy for all.⁵⁷
- Ahmad Dhani, an Indonesian rock star, has used both his music and his stardom to counter calls to violence with a message of peace and tolerance. His 2004 album, titled “Laskar Cinta” (Warriors of Love) was a direct challenge to “Laskar Jihad” (Warriors of Jihad), a violent militia in Indonesia.⁵⁸

Jordan.

- In July 2005, 170 leading Muslim clerics issued a *fatwa* (Islamic legal pronouncement) in Amman denouncing all acts of terrorism committed in the name of Islam. A little known but notable fact, the fatwa was issued a day before the bombings in London on 7/7.⁵⁹

Saudi Arabia.

- Public television aired a five-part series titled “Jihad Experiences: The Deceit.” Among other things, the series featured renunciations of terrorism by former “jihadists.” The series also showcased scholarly rebuttals to extremist propaganda.⁶⁰
- Huge banners and signs have been hung throughout the capital to illustrate the human costs of terrorism.⁶¹ Similar broadcasts have occurred on television and even on the screens of automated teller machines.

⁵⁵ Fawaz A. Gerges, “The End of the Islamist Insurgency in Egypt?: Costs and Prospects,” *The Middle East Journal* (Autumn 2004): 594.

⁵⁶ “Women Have Equal Rights in Islam and Can Be Rulers,” *Gulf News*, February 5, 2007, <http://archive.gulfnews.com/articles/07/02/05/10101999.html>.

⁵⁷ See LibforAll Foundation <<http://www.libforall.org/home.html>>.

⁵⁸ Daveed Gartenstein-Ross, “Warrior of Love: An Unlikely Champion of Moderate Islam,” *The Weekly Standard*, November 15, 2006, <http://www.weeklystandard.com/Content/Public/Articles/000/000/012/932fifqs.asp?pg=1>.

⁵⁹ Kenneth Ballen, “The Myth of Muslim Support for Terror,” *The Christian Science Monitor*, February 23, 2007, <http://www.csmonitor.com/2007/0223/p09s01-coop.html>.

⁶⁰ See “TV Seminar Offers an Overview of the Series titled Jihad Experiences,” *Al-Riyadh Newspaper*, Issue No. 13700, December 27, 2005, <http://www.alriyadh.com/2005/12/27/article118422.html>. See also “TV broadcasts a five part series titled ‘Jihad Experiences, the Deceit...’,” *Al-Riyadh Newspaper*, Issue No. 13672, November 25, 2005, <http://www.alriyadh.com/2005/11/29/article111369.html>.

- The Interior Ministry is developing a plan (to include lectures and seminars) to portray extremist “jihadi” Salafism as a deviant form of Islam to students in schools and universities.⁶² Textbooks and curriculum are being audited to ensure that schools are not used to radicalize students.⁶³
- As part of a government-supported “Tranquility Campaign,” volunteers including scholars of religion, psychiatrists, and sociologists have visited websites, chat rooms and forums to engage in dialogue with extremists. According to government figures, almost 700 individuals have recanted their beliefs as a result. As part of the Campaign, there is an ongoing effort to establish a website to help counter extremist ideology.⁶⁴
- Under a new law to fight cyber-crime, approved on April 13, 2007, it is a punishable offence (up to ten years in prison and/or a fine of up to 5 million Saudi riyal, which equates to approximately \$1.3 million) to create a website for a terrorist organization.⁶⁵

United States.

- Immediately following September 11, 2001, a fatwa condemning terrorism and extremism was issued by American Muslim jurists and ultimately was endorsed by more than one hundred and twenty U.S. Muslim groups, leaders and institutions. The fatwa deemed terrorism or involvement in terrorism by any individual or group as *haram* (forbidden) and stated “it is the civic and religious duty of Muslims to cooperate with law enforcement authorities to protect the lives of all civilians.”⁶⁶
- In 2005, the Fiqh Council of North America, comprised of Islamic scholars from the United States and Canada, issued a fatwa against terrorism and extremism.⁶⁷
- “The American Muslim,” an online journal, seeks to highlight the voices of Muslims who have spoken out against terrorism and extremism. The magazine describes the latter voices as “the Muslim majority who don’t get publicity.”⁶⁸
- Another venture, “On the Road in America,” is a reality series produced in the U.S. and licensed to broadcasters in the Middle East. The show features “a caravan of

⁶¹ Christopher Boucek, “Saudi Security and the Islamist Insurgency,” *Terrorism Monitor*, January 26, 2006, <http://jamestown.org/terrorism/news/article.php?articleid=2369879>.

⁶² Mariam Al Hakeem, “Saudi Arabia’s Anti-Terrorism Campaign to Target Students,” *Gulf News*, November 22, 2006, http://archive.gulfnews.com/region/Saudi_Arabia/10084291.html.

⁶³ See Christina Bellantoni, “Islamic groups hit curriculum at Saudi school,” *The Washington Times*, August 2, 2004, <http://www.washingtontimes.com/functions/print.php?StoryID=20040802-123606-9597r>. See also “Counter-Terrorism International Conference” (report of conference in Riyadh, Saudi Arabia, February 5-8, 2005), <http://saudiembassy.net/ReportLink/terrorism-CTIC-overview-Feb05-Q.pdf>.

⁶⁴ See Appendix A.

⁶⁵ Ibid.

⁶⁶ Ibid.

⁶⁷ Jason DeRose, “U.S. Muslim Scholars Issue Edict Against Terrorism,” *NPR All Things Considered*, July 28, 2005, <http://www.npr.org/templates/story/story.php?storyId=4775588>.

⁶⁸ Sheila Musaji, et. al., “Muslim Voices Against Extremism and Terrorism,” *The American Muslim*, December 8, 2006, http://theamericanmuslim.org/tam.php/features/articles/muslim_voices_against_extremism_and_terrorism_part_i_fatwas/0012209.

- young...Arabs crisscrossing America on a mission to educate themselves and the people they encounter along the way.”⁶⁹
- The Terrorism Research Center monitors the Internet for insights into a range of matters including terrorists’ “world view, beliefs and strategies”; this information is compiled in a weekly report titled “Terror Web Watch.”⁷⁰
 - In 2005, the Muslim Public Affairs Council released the *Grassroots Campaign to Fight Terrorism Handbook*. The text is intended to serve as an informational resource for a wide audience, from imams and Muslim leaders to law enforcement and media.⁷¹
 - Within government, the Department of Homeland Security (DHS)’s Office for Civil Rights and Civil Liberties has produced “an intensive training DVD for DHS personnel who interact with Arab Americans, Muslim Americans, and people from the broader Arab and Muslim world.” The logic underlying this tool is simple but forceful, namely, that members of these communities will “be treated with more dignity and professionalism if front-line officers understand their cultures, traditions and values...”⁷²

Yemen.

- The government-developed Committee for Dialogue, composed of senior clerics and ministers, is tasked with eliminating extremism through debate. Using only the Qur’an and the Sunnah (the recorded traditions of the Prophet Muhammad, both decisions and practices) as a foundation, members of the Committee attempt to convince imprisoned extremists that there is no basis in Islam for terrorism. Those who accept the clerics’ arguments are re-integrated into Yemeni society; according to the government, as of June 2005, 364 individuals had been rehabilitated and released.⁷³

A more robust counter-strategy is needed, however – one that builds on best practices above, but is more comprehensive in nature. Weaving these disparate efforts into a more coherent and powerful international campaign, in part by building on the synergies that may exist between and among these many and varied initiatives, will require ingenuity and resolve on the part of all concerned.

⁶⁹ Jacques Steinberg, “American Road Trip Through Arab Eyes.” *The New York Times*, January 21, 2007, <http://www.nytimes.com/2007/01/31/arts/television/31road.html>.

⁷⁰ See Terror Web Watch, *Terrorism Research Center*, <http://www.terrorism.com/modules.php?op=modload&name=About&file=index&subcontent=products&detail=strategicreports>.

⁷¹ Full text available at <http://www.mpac.org/publications/campaign-to-fight-terrorism/campaign-to-fight-terrorism-brochure.pdf>.

⁷² Daniel W. Sutherland, “Threat of Islamic Radicalization to the Homeland,” testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, March 14, 2007, p. 7.

⁷³ Michael Tarnby, “Yemen’s Committee for Dialogue: Can Jihadists Return to Society?” *Terrorism Monitor*, July 15, 2005, <http://www.jamestown.org/terrorism/news/article.php?articleid=2369745>.

Counter-Strategy: Guiding Principles and Key Challenges

Extremists have come to value the Internet so highly that some “jihadists” have adopted the slogan “keyboard equals Kalashnikov.”⁷⁴ Denying or disrupting their access to the Internet is easier said than done effectively, however. In certain circumstances, it may be possible to invoke the law as a blunt instrument to shut our adversaries down. This would be the case when extremist websites directly incite violence or provide material support to known terrorist organizations, thereby crossing the line from constitutionally protected speech into illegal acts. In other instances, technical means could be used to knock our adversaries off balance. The U.S. Air Force, for instance, has announced plans to create a Cyber Command which will, among other things, “work to defeat terrorists by disrupting...the Web sites they create for training and recruiting.”⁷⁵

As a practical matter, though, it is difficult to squelch an extremist presence online. A website targeted in one country can often simply move to a new server in another. Indeed, some groups change their server daily. Like a game of whack-a-mole, you may knock down one site only to find another pop up elsewhere. The analogy is imperfect however, because the offending online material may not be so easy to spot. Extremists may go to great lengths to mask their activities online, such as concealing materials by fragmenting, encrypting and scattering them across a number of different websites.

Conversely, much extremist material is openly available and officials have already begun to exploit this intelligence, often using commercial software to monitor targeted websites.⁷⁶ Treasure troves of data may also be contained in computers that are seized by U.S. forces during raids. Yet those finds may not be fully plumbed in part because it is “a daunting challenge” to “find...analysts who understand [both] forensic computer jargon as well as counterterrorism.”⁷⁷ A number of U.S. government entities engage in “digital forensics” work of this sort, but the largest effort is that of the Pentagon’s Cyber Crime Center, which supports counterterrorism efforts as well as criminal investigations.⁷⁸

Open source intelligence (or that garnered by other means) that reveals what extremists are saying to one another, and to others they hope to radicalize, is a crucial input for counter-strategy. **There can be no compelling counter-narrative until the extremist narrative itself is well understood** – including how that message is couched, what is emphasized and ignored, what references and allusions are made, what audiences are targeted, and how messages are adapted to reach new audiences and respond to new events. To the extent that government officials are involved in gathering and/or interpreting this information, efforts

⁷⁴ See Appendix A.

⁷⁵ Josh Rogin, “Air Force to Create Cyber Command,” *FCW.com*, November 13, 2006, <http://www.fcw.com/article96791-11-13-06-Print>.

⁷⁶ Conway, *supra* note 54 at p. 23.

⁷⁷ Siobhan Gorman, “Tracking Terrorists With Click of a Mouse,” *The Baltimore Sun*, March 27, 2007, <http://www.baltimoresun.com/news/nationworld/bal-te.forensic26mar26,0,620050.story?coll=bal-pe-asection>, citing Evan Kohlmann.

⁷⁸ *Ibid.*

will be hampered by the paucity of Arabic language skills in the workforce (the vast majority of extremist websites that are of interest in this context are either wholly or partly in Arabic).⁷⁹ Nuances in meaning may also be lost due to a lack of cultural understanding. Until Arab-Americans and other diverse groups are sufficiently encouraged and actually choose public service as a career, this problem will persist.

Covert work alluded to above, may yield results as is true in the context of other criminal investigations. Through careful and patient effort, it is possible that an intelligence officer posing as a sympathizer could infiltrate an online extremist community. While remaining cognizant of civil liberties, “[t]he public nature of...chat rooms mitigates the need for informed consent.”⁸⁰ Seeds of confusion, doubt and distrust could then be planted in order to chip away at the ties that bind individual extremists into a cohesive and dangerous group. Terrorist susceptibility to psychological manipulation should not be discounted or underestimated. The infamous Abu Nidal, for instance, was ultimately brought down by such measures, which fostered and magnified concerns in his own mind about the loyalty and discipline of those surrounding him.

“Honey pots” or websites which resemble extremist sites could also be created to further the spread of disinformation. The possibilities here are vast, limited only by our imagination and already thinly stretched resource levels in the intelligence community. Activities of this sort do, of course, run the risk of generating “blowback” (in the layman’s sense of the term) if they are ultimately discovered and exposed. For this reason, it is important to reflect thoughtfully, ahead of time, upon the various potential costs and benefits that may be associated with the action(s), and assess (to the extent possible in advance) whether a net gain is likely to result. Measures to mitigate the impact of possible blowback before it even materializes could also be undertaken in tandem with (or prior to) covert activity. Demonstrating restraint in certain other policy areas that are presently irritants or sources of friction may permit some of the high ground to be recaptured.⁸¹

The larger issue centers on how it is that a nation that gave rise to Silicon Valley, Hollywood, and Madison Avenue came to be outplayed in the realm of ideas, effectively communicated in the new media. Part of the answer is that we have not yet really applied our collective talents and energies to the problem. Domination of the battlefield is not much of a feat when the contest is one-sided because one party defaulted by failing to show. Moreover, it will require international collaboration because transnational challenges require transnational responses.

Fundamentally, the challenge is one of containment and ultimately rollback – of an idea – or more precisely, a collection of ideas that have been packaged into a compelling narrative and effectively marketed. Therefore, we should look to the subject who is, or who eventually becomes, responsive to these ideas as well as those who do not (the control group). The behavioral science underlying that receptivity and/or vulnerability to the messaging should

⁷⁹ See Appendix A.

⁸⁰ Glaser, Dixit, and Green, *supra* note 21 at p. 190.

⁸¹ See Appendix A.

give rise to possible points of intervention, where the process of radicalization could be halted in its tracks.

Another and more important piece of the explanation is that the solution to the problem simply does not lie firmly within our grasp. Instead, part of the solution lies within Islam itself. Unless both the counter-messages and those who deliver it come from within, the counter-narrative will be deemed inauthentic and untrustworthy, and will fail to resonate. While there may be a role for governments to play by helping, at arm's length, to amplify these voices emanating from the grassroots level, the trick lies in figuring out how to do so without tainting the credibility of either the message or the messenger.

What follows is not a detailed roadmap of highly specific actions that should be taken by particular agencies or entities, in priority order, over a precise time frame. Instead, a range of ideas are proposed to guide our response postures both online and offline, and heighten their effectiveness. These suggestions are informed by three key themes: how and why individuals are influenced via CMC; the need to counter extremist speech with an effective counter-narrative that challenges extremist ideology and also offers an alternative to those who are currently feeling alienated and marginalized; and the importance of intelligence work to inform counterterrorism and the counter-narrative. Some of the recommended ideas are more theoretical and are therefore intended to serve as conceptual foundations or underpinnings for action. Other ideas are quite granular and are offered in a more focused and “mechanical” spirit, as a suggested fix or pinpoint prescription. Against this background, the following five-pronged plan is suggested:

Key Recommendations

1. Craft a Compelling Counter-Narrative for Worldwide Delivery, in Multimedia, At and By the Grassroots Level

Challenge extremist “doctrine.” The global extremist “jihadi” Salafist movement propagates misinformation and distorts genuine theological tenets for the purpose of expanding the movement’s ranks and energizing its base. These myths and falsehoods must be debunked and discredited. The West is not engaged in battle against Islam. Terrorism is un-Islamic. The price paid in blood by Muslims has been high: “Muslim terrorists have usually killed more Muslims than Jews or Christians.”⁸² Koranic passages such as “the sword verse” (9:5) are wrongly invoked to justify acts of aggression.

⁸² Christopher C. Harmon, “The Myth of the Invincible Terrorist,” *Policy Review* (April/May 2007): p. 10, <http://www.hoover.org/publications/policyreview/6848137.html>.

Offer a compelling narrative that pulls potential extremists back from the brink. A narrative will only appeal if it resonates with an individual's personal experience. Creation and distribution of a counter-narrative should not be confused with efforts to improve America's image. Rather, the counter-narrative should offer a "dream" in the form of hope and realistically attainable alternative futures to those who might otherwise be seduced by the lure of extremist ideology.

Use graphic visuals to magnify the impact of language. Footage of dead children. Images of the carnage of other innocents whose lives were cut short by terrorism. Distasteful as this may be to invoke, the power of visuals is profound. They can enhance exponentially the impact of the written or spoken word. Our adversaries have not hesitated to rely on this tactic to inspire others to join the extremist cause. Where appropriate, we should fight fire with fire.

Build on core values common to all. Non-extremists everywhere, no matter their religious or political stripe, hold dear certain universal values such as "respect for the law, freedom of speech, equality of opportunity, respect for others, and responsibility towards others." What unites us is indeed greater than what divides us⁸³ and the counter-narrative must emphasize this crucial point.

Authentic sources must deliver the message. Unless elements of the counter-narrative emanate from within the Muslim community and are conveyed by voices that are trusted and credible within those communities, the opportunity to achieve impact will be limited at best. For example, Radio Free Europe was created by and for Polish dissidents who possessed a thorough understanding of the many facets of the issues at play and could use effective satire as part of their counter-narrative. Another authentic messenger may, in fact, be former extremists who repudiate those beliefs and may be valuable to the counter-messaging effort. Consider as a model the HBO documentary film titled "Bastards of the Party" (2006), featuring ex-members of Los Angeles' street gangs condemning and rejecting their previous existence. Testimonials and renunciations (in the context of the extremist belief system under present study), broadcast on television or the Internet, may prove persuasive and resonate with youth in particular.⁸⁴ More recently, "60 Minutes" aired a segment in which Hassan Butt, once a recruiter for al Qaeda in the United Kingdom, repudiated his former existence. Specifically, his role was one of recruiting individuals for the 7/7 bombings.⁸⁵

Amplify and augment non-extremist voices emanating from the grassroots. Many Islamic clergy members and scholars have stated, for instance, that Islam expressly forbids attacks against civilians and suicide bombings. However, these and other messages of

⁸³ Ruth Kelly, "Britain: Our Values, Our Responsibilities," speech by United Kingdom Communities Secretary, October 11, 2006, <http://www.communities.gov.uk/index.asp?id=1503690>.

⁸⁴ See "Bastards of the Party," produced by Antoine Fuqua and Cle Sloan, HBO, February 6, 2007, <http://www.hbo.com/docs/programs/bastardsoftheparty/index.html>.

⁸⁵ See 60 Minutes, "The Network," produced by Michael Gavshon, CBS, March 25, 2007. See also "The Network: Hassan Butt Tells Bob Simon Killing in The Name of Islam Is a 'Cancer'," CBS, March 25, 2007, <http://www.cbsnews.com/stories/2007/03/23/60minutes/main2602308.shtml>.

moderation are simply not being heard and noticed to the same degree as their extremist counterpart. More such speech is needed and, to magnify it, resources should be provided where necessary.

2. Foster Intra- and Cross-Cultural Dialogue and Understanding to Strengthen the Ties that Bind Together Communities at the Local, National, and International Levels

Address perceptions and realities of American Muslim alienation and marginalization. In a Washington Post “On Faith” blog to promote his new book, *Religious Literacy: What Every American Needs to Know – And Doesn’t*, Stephen Prothero argues that “the United States may be one of the most religious nations on earth but Americans know woefully little about their own religions, or the religions of others.”⁸⁶ Such ignorance has profound implications as we seek to increase dialogue and further integrate Muslim communities within the U.S. The genuine sense of alienation and marginalization that many Muslims in the United States feel must be addressed. Greater civic engagement of Muslim communities will further enable integration as appropriate. It is important to note that all of this takes place within the larger context of the public square, where cultural and religious knowledge in general is lacking.

Civic Engagement. Democracies are by their very nature inclusionary, and national and domestic security policy debates, forums, and activities will benefit by ensuring that American Muslims are part of such discussions. At the federal level, a promising, yet underfunded and under-resourced effort is that of the DHS Office for Civil Rights and Civil Liberties. Responsible for engaging with American Arab and Muslim communities nationwide, the Office has only a Director and two full-time employees. At the community level, examples of civic engagement include involvement of American Muslims in efforts to “Train the Trainers” in Community Emergency Response Training (CERT) in the state of Michigan. A first step was to translate the CERT Instructor Guide into Arabic. Another model of engagement with Muslim communities is the Tulsa, Oklahoma Citizen Corps Council’s Language – Cultural Bank that brings together individuals with foreign language skills or multicultural experiences in a volunteer capacity to assist community agencies with disaster response, emergency preparedness, and crisis management.

People to People Exchanges. While more pronounced in Europe, Muslim communities on both sides of the Atlantic share feelings of estrangement. A successful bilateral approach to further efforts to promote cross-cultural understanding was that of the U.S. Embassy in Brussels and the Belgian Royal Institute’s conference with Belgian and American Muslims titled “Muslim Communities Participating in Society: A Belgian-U.S. Dialogue.” Initiated by Ambassador Tom Korologos, and co-sponsored by the Royal Institute for International Relations, the conference used mediated dialogue “to

⁸⁶ Stephen Prothero, “Another Amen for Religious Liberty,” On Faith blog, posted March 19, 2007, http://newsweek.washingtonpost.com/onfaith/guestvoices/2007/03/another_amen_for_religious_lib.html.

work together to break stereotypes and foster networking opportunities” with the goal of identifying best practices “for improving the participation of Muslim communities in Belgian and American societies.”⁸⁷

Role of the Media. The media can play a major role by covering stories and events when groups speak out against extremist elements and messaging, and by taking care to use Islamic terms appropriately.

3. Recognize and Address the Need for Additional Behavioral Science Research into the Process of Radicalization both Online and Offline

Deepen our understanding of the process of radicalization to further inform counter-strategy. Greater study of the process of radicalization is needed, in part to identify trigger points and possible points of intervention. This will require a multi-disciplinary approach, drawing on experts in fields ranging from sociology to psychology to religion to socio-economics to law enforcement.

Apply social networking theory. Social network analysis will serve as an important tool to assist us in making sense of the various connections within a terror network. As one former analyst explains, “[t]errorist organizations do not have organizational charts, they have relationships and if you can understand those relationships, you have gained valuable intelligence.”⁸⁸

4. Deny or Disrupt Extremist Access to, and Extremist Efforts through, the Internet via Legal and Technical Means, and Covert Action, Where Appropriate

Invoke the full force of the law where it makes most sense to do so. Legal means for disrupting extremist use of the Internet may be useful against websites that directly advocate violence or provide material support to known terrorist organizations, crossing the line from protected speech to illegal acts of violence.

The convergence of human intelligence and cyberspace must be fully appreciated and skillfully exploited in the Information Age. The intelligence community should work to gather information about extremist groups through their online activities, and act – at an appropriate or judicious time – to disrupt the plans of those plotting acts of violence. More intelligence officers are needed and for a range of purposes, to include infiltrating chat rooms, recruiting individuals and conducting false flag operations.

⁸⁷ See Appendix A.

⁸⁸ Bender, *supra* note 49, citing Montgomery McFate, former Navy analyst.

Undermine the trust that binds enemy networks. “Honey pot” websites that resemble the extremists’ own would simultaneously permit the gathering of information about visitors to the site while enabling counterterrorism personnel to sow the seeds of doubt and distrust among extremists. Honey pots could allow us to better understand how local political grievances can become appropriated by the global extremist “jihadi” Salafist movement, which in turn can inform a counter-strategy to drive wedges between and among factions, thereby playing on existing fault lines.

5. Remedy Resource and Capability Gaps in Government

Address deficits in linguistic and cultural knowledge, skills and abilities. The ability to speak, understand and translate Arabic is crucial to prevention and response efforts, yet U.S. government capacities in that regard are much weaker than they should be.

Choose words carefully to reclaim the high ground. Ill-chosen words and expressions by governments and institutions are used in extremist propaganda to further radicalize potential adherents. We have ceded the high ground to terrorist networks by adopting their preferred vocabulary, and thereby inadvertently serving their interests. In crafting a counter-narrative, words and concepts must be chosen carefully to avoid bestowing on our adversaries qualities such as honor and nobility that they so clearly do not embody. The European Union has taken a step in trying to more clearly define such terms by producing non-binding guidelines that pertain to matters of lexicon. The intent is to “prevent the distortion of the Muslim faith and the alienation of Muslims in Europe.”⁸⁹ The effectiveness of this measure has yet to be determined.

Remedy the lack of a strategic communications plan. There currently exists no comprehensive well-informed strategy for effectively articulating an anti-extremist message. The U.S. State Department has a “small digital outreach team,” which “monitor[s] Arabic political discussion forums on the Internet and...overtly participate[s] in them in an effort to correct misperceptions about U.S. policy in the Middle East.”⁹⁰ But no single organization or institution either within the government or outside of it is capable of managing this effort alone. Instead, a network of networks must be established that links and coordinates efforts by a variety of actors, both public and private. Multiple government agencies must be budgeted according to their mission in order to build an anti-extremist messaging capability. Unlike the Office of War Information established during World War II and vested with the responsibility and authority to coordinate and oversee counter-messaging efforts, in this instance a more decentralized approach is required.

Expand community policing programs. At the local level, law enforcement must develop new relationships and deepen existing ones within Muslim communities. Local figures

⁸⁹ Bruno Waterfield, “Don’t confuse terrorism with Islam, says EU,” *The Daily Telegraph*, March 30, 2007, <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/03/30/wislam30.xml>.

⁹⁰ Nicholas Kralev, “Arabic speakers monitor Net chats,” *The Washington Times*, March 9, 2007, <http://www.washtimes.com/world/20070308-111426-4682r.htm>.

NETWORKED RADICALIZATION: *A Counter-Strategy*

are best placed to identify radicalization at its earliest stages. Cultivated mutual respect and understanding between officials and communities, founded on a solid education about Muslim cultures and Islam, is crucial.

Appendix A

Task Force on Internet-Facilitated Radicalization Briefings*

- Geneive Abdo: Senior Analyst, Gallup Center for Muslim Studies
- Parvez Ahmed: Chairman of the Board, Council on American-Islamic Relations (CAIR)
- David Carment: Associate Professor of International Affairs, Norman Paterson School of International Affairs, Carleton University, Ottawa
- Jim Dempsey: Policy Director, Center for Democracy and Technology
- Anna Gray: Director General, Intelligence Requirements & Strategic Integration, Royal Canadian Mounted Police National Security Investigations
- Tom Korologos: Former U.S. Ambassador to Belgium
- Jeffrey Lang: Author and Professor, University of Kansas
- Mike McDonnell: Assistant Commissioner, National Security Investigations, Royal Canadian Mounted Police
- Fuad Nahdi: Founding Editor, Q News
- Bruno Nordeste: Program Officer, CANADEM, Canada's Civilian Reserve
- Lidewijde Ongering: Deputy Coordinator for Counterterrorism, Netherlands
- Reuven Paz: Director, Project for the Research of Islamist Movements (PRISM)
- William Pelgrin: Director, Office of Cyber Security and Critical Infrastructure, New York
- Dennis Pluchinsky: Former U.S. State Department Intelligence Analyst
- Marc Sageman: Sageman Consulting
- Anna Stenersen: Norwegian Defense Research Establishment
- Daniel Sutherland: Officer for Civil Rights and Civil Liberties, Department of Homeland Security

-
- Peter Swire: C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University
 - Truls H Tønnessen: Norwegian Defense Research Establishment

* The task force consulted, interviewed and received briefings from additional subject matter experts who wish to remain anonymous. All briefings were conducted under "Chatham House" rules.

Appendix B

Additional Resources

- Abdo, Geneive. *Mecca and Main Street: Muslim Life in America After 9/11*. Oxford University Press, 2006.
- Ahmed, Parvez. "Terror in the Name of Islam: Unholy War not Jihad." Paper presented at the 'Sacred Violence: Religion and Terrorism' conference held by the Institute for Global Security, Law and Policy at the Case Western University School of Law, Cleveland, Ohio, March 30, 2007.
- Allen, Charles E. "Threat of Islamic Radicalization to the Homeland." Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, March 14, 2007, http://hsgac.senate.gov/_files/031407Allen.pdf.
- "Al-Qaeda online: understanding jihadist internet infrastructure." *Jane's Intelligence Review* (January 1, 2006).
- Aslan, Reza. *No god but God: The Origins, Evolution, and Future of Islam*. Random House, 2005.
- Ballard, James David, et al. "Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues." *American Behavioral Scientist* 45, no. 6 (2002): 989-1016.
- BBC Monitoring. "Romanian President Calls for Responsible, Moral Use of Internet." *BBC Monitoring International Reports*, December 10, 2003.
- Bowers, Faye. "Terrorists Spread Their Messages Online; A Growing Number of Al Qaeda Websites Offer Instructions for Kidnapping and Killing Victims." *Christian Science Monitor*, July 28, 2004, p. 3.
- Brandon, James. "Internet Jihad: Tackling Terror on the Web; A British Citizen Faces US Charges for Running a Militant Site Hosted in Connecticut." *Christian Science Monitor*, February 3, 2006, p. 6.
- Buchanan, Mark. *Nexus: Small Worlds and the Groundbreaking Theory of Networks*. W. W. Norton & Company, 2003.
- Canadian Centre for Intelligence and Security Studies. "A Framework for Understanding Terrorist Use of the Internet," *Trends in Terrorism* 2 (2006).
- Celeste, Sofia. "Want to Check Your E-mail in Italy? Bring your passport." *Christian Science Monitor*, October 4, 2005, p.7.

-
- Cherry, Steven. "Terror Goes Online." *IEEE Spectrum* 42, no. 1 (2005): 72-73.
- Chertoff, Michael. "Threat of Islamic Radicalization to the Homeland." Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, March 14, 2007, http://hsgac.senate.gov/_files/031407Chertoff.pdf.
- Cilluffo, Frank and J. Paul Nicholas, "Cyberstrategy 2.0." *Journal of International Security Affairs* 10 (2006), http://www.gwumc.edu/hspi/pubs/Cilluffo_cyberstrategy.pdf.
- Coll, Steve and Susan Glasser. "Terrorists Turn to the Web as Base of Operations." *The Washington Post*, August 7, 2005, p. A1.
- Conway, Maura. "Reality Bytes." *First Monday* 7, no. 11 (2002), http://www.firstmonday.org/issues/issue7_11/conway/index.html.
- Conway, Maura. "Terrorism and the Internet: New Media – New Threat?" *Parliamentary Affairs* 59, no. 2 (2006): 1-16.
- Counterterrorism Blog. <http://counterterrorismblog.org/>.
- Cronin, Audrey Kurth. "Cyber-Mobilization: The New *Levée en Masse*." *Parameters* 36, no. 2 (2006): 77-87.
- Dagnes, Alison D. "White noise: The political uses of Internet technology by right-wing extremist groups." PhD diss., University of Massachusetts Amherst, 2003.
- Etter, Sr., Gregg W. "Security Threat Groups: The Threat Posed by White Supremacist Organizations." *Journal of Gang Research* 10, no. 2 (2003): 1-24.
- Fallows, James. "Declaring Victory." *The Atlantic Monthly*, September 2006, http://www.theatlantic.com/doc/200609/fallows_victory/.
- Faria, João Ricardo and Daniel G. Arce M. "Terror Support and Recruitment." *Defence and Peace Economics* 16, no. 4 (2005): 263-273.
- Fattah, Hassan M. "Growing Unarmed Battalion in Qaeda Army Is Using Internet to Get the Message Out." *The New York Times*, September 30, 2006, p. A.6.
- Hamilton, Lee and Frank J. Cilluffo, "Report of the Future of Terrorism Task Force." Homeland Security Advisory Council, January 2007. <http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf>.
- Hammes, Thomas. "Safe Havens and Cyberspace." *Jane's Defence Weekly*, October 2005.

Hara, Noriko and Zilia Estrada. "Analyzing the Mobilization of Grassroots Activities via the Internet: A Case Study." *Journal of Information Science* 31, no. 6 (2005): 503-514.

"The Homeland Security Implications of Radicalization." Hearing before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, September 20, 2006.

Jenkins, Brian Michael. "Building an Army of Believers: Jihadist Radicalization and Recruitment." Testimony before the U.S. House of Representatives Homeland Security Committee, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, April 5, 2007, http://www.rand.org/pubs/testimonies/2007/RAND_CT278.pdf.

"Jihad Online: Islamic Terrorists and the Internet." Anti-Defamation League, http://www.adl.org/internet/jihad_online.pdf.

Kohlmann, E.F. "The Real Online Terrorist Threat." *Foreign Affairs* 85, no. 5 (2006), www.foreignaffairs.org/20060901faessay85510/evan-f-kohlmann/the-real-online-terrorist-threat.html.

Kramer, Rachel. "Internet use by terrorists and content analysis of terrorist websites." M.A. diss., University of London, 2003.

Labi, Nadya. "Jihad 2.0." *The Atlantic Monthly* 297, no. 6 (2006): 102-108.

Lee, Elissa and Laura Leets. "Persuasive Storytelling by Hate Groups Online." *American Behavioral Scientist* 45, no. 6 (2002): 927-957.

Levin, Brian. "Cyberhate – A Legal and Historical Analysis of Extremists' Use of Computer Networks in America." *American Behavioral Scientist* 45, no. 6 (2002): 958-988.

Lynch, Marc. Abu Aardvark. <http://abuaardvark.typepad.com/>.

National Coordinator for Counterterrorism. "Jihadis and the Internet." Netherlands Ministries of Justice and of the Interior and Kingdom Relations, February 2007. http://english.nctb.nl/Images/Jihadis%20and%20the%20Internet_tcm127-139397.pdf

Paz, Reuven. "Reading Their Lips: The Credibility of Jihadi Web Sites in Arabic as a Source for Information." Project for the Research of Islamist Movements. www.e-prism.org/images/Read_Their_Lips.doc.

Philips, Kyra, et al. "Multiple al Qaeda-Friendly Sites Being Dropped." *CNN News*, May 13, 2004, <http://transcripts.cnn.com/TRANSCRIPTS/040513/lol.02.html>.

-
- “Prison Radicalization: Are Terrorist Cells Forming in U.S. Cell Blocks?” Hearing before the U.S. Senate Homeland Security and Governmental Affairs Committee, September 19, 2006, <http://www.senate.gov/-govt-aff/index.cfm?Fuseaction=Hearings.Detail&HearingID=397>.
- Qin, Jialun, et al. “Unraveling international terrorist groups’ exploitation of the Web: technical sophistication, media richness, and Web interactivity.” Paper presented at the annual Intelligence and Security Informatics International Workshop, Singapore, April 9th, 2006.
- Rajawat, K. Yatish and Ritwik Donde. “Mumbai Cops to Invade Cyberspace.” *Economic Times*, September 23, 2006.
- Reid, Edna, et al. “Collecting and Analyzing the Presence of Terrorists on the Web: A Case Study of Jihad Websites.” *Intelligence and Security Informatics* 3495 (2005): 402-411.
- Rogan, Hanna. *Jihadism Online: A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes*. Kjeller, Norway: Norwegian Defence Research Establishment, 2006.
- Rogan, Hanna. *The London Bombings.com: An Analysis of Jihadist Website Discussion about the Attacks*. Kjeller, Norway: Norwegian Defence Research Establishment, 2005.
- Sageman, Marc. *Leaderless Jihad*. Philadelphia: University of Pennsylvania Press, 2007.
- Stanton, John J. “Terror in Cyberspace.” *American Behavioral Scientist* 45, no. 6 (2002): 1017-1032.
- Stephens, Hampton. “Hosting Terror.” *Foreign Policy* 155 (2006): 92.
- Sutherland, Daniel W. “Threat of Islamic Radicalization to the Homeland.” Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, March 14, 2007, http://hsgac.senate.gov/_files/031407Sutherland.pdf.
- Taylor, Peter. 2005. Web of Terror. *Mail on Sunday*, July 24.
- Tessler, Mark and Michael D. H. Robbins. “What Leads Some Ordinary Arab Men and Women to Approve of Terrorist Acts Against the United States?” *Journal of Conflict Resolution* 51, no. 2 (2007): 305-328.
- Thomas, Timothy L. “Al Qaeda and the Internet: The Danger of ‘Cyberplanning.’” *Parameters* 33, no. 1 (2003): 112-123.
- Tibbetts, P.S. “Terrorist Use of the Internet and Related Information Technologies.” Unpublished paper, Army Command and General Staff College, School of Advanced Military Studies. Fort Leavenworth, KS, 2002.

Timmons, Heather and Eric Pfanner. "Threats and Responses: Security; Europe Says It Will Unify Effort in Fight on Terrorism." *The New York Times*, August 17, 2006, final edition, p. 15.

Tsfati, Yariv. "www.terrorism.com: Terror on the Internet." *Studies in Conflict & Terrorism* 25, no. 5 (2002): 317-332.

"Ukraine Bans Web-based Terror Propaganda." *Interfax*, December 9, 2003.

Verton, Dan. "Al-Qaeda Poses Threat to Net." *Computerworld* 26, no. 48 (2002): 1, 14.

Weimann, G. "Virtual Disputes: The Use of the Internet for Terrorist Debates." *Studies in Conflict & Terrorism* 29, no. 7 (2006): 623-639.

Westfeldt, Amy. "Rumsfeld Says Extremists Are Beating U.S. Government to the Punch in Media War." *AP Worldstream*, February 17, 2006.

Wright, Lawrence. "The Terror Web." *The New Yorker*, August 2, 2004.

Zhou, Y.; Reid, E.; Qin, J.; Chen, H.; Lai, G. 2006. "U.S. Domestic Extremist Groups on the Web: Link and Content Analysis." *IEEE Intelligent Systems*, Vol. 20, No.5. pp. 44-51.