Center on Global Counterterrorism Cooperation

POLICY BRIEF
February 2011

Use of the Internet for Counter-Terrorist Purposes

Liat Shetret

Introduction

On 1 May 2010, Faisal Shahzad, a naturalized U.S. citizen, tried to detonate a car bomb in the heart of New York's Times Square. Thanks to the vigilance of local witnesses and to technical shortcomings, the bomb was detected and failed to explode. The investigation surrounding Shahzad's case, like other, more recent cases,[1] shows that the Internet played an important role in his violent radicalization and the planning and execution of the attempted attack. For example, he drew spiritual inspiration from lectures and videos circulated online by Anwar al-Awlaki, a U.S.-Yemeni cleric, who helped to convince Shahzad to take up the cause of al-Qaida.[2] Shahzad accessed Web sites for operational and planning purposes. He viewed "real-time video feeds of different areas of Times Square" to help determine which areas attract a large crowd and would result in a high casualty rate if attacked.[3] Shahzad also used the Internet to discuss his plans with militants based in Pakistan.[4]

Terrorist operatives such as Shahzad often draw inspiration, reinforcement, support, and guidance from a variety of on- and off-line sources. Some clerics; experts; scholars, such as al-Awlaki; and virtual communities use the Internet to promote violent extremism on their blogs, social network pages, discussion forums, or through the streaming of videos on multimedia platforms such as YouTube.[5] This brief provides an overview of challenges posed to stakeholders by the use of the Internet for terrorist purposes. It argues that the Internet is not the problem and that the online platform can be employed to counter terrorism efforts. Specifically, models of violent radicalization processes off-line offer an important and useful framework for the development and implementation of policies to counter online use of the Internet for terrorist purposes.[6]

The brief concludes by offering multilateral institutions, states, civil society organizations, the media, and the private sector examples of how they can use the Internet more effectively as a counterterrorism tool to prevent and counter the use of the Internet for violent radicalization. Four intervention points are suggested: (1) weaken cult personalities, (2) challenge the extremist doctrine, (3) dispel the glory of the "terrorist lifestyle," and (4) offer a street-smart and locally developed and communicated counternarrative.

Background

The Internet is a medium that facilitates the maintenance of a decentralized, global, violent extremist movement. It provides a virtual forum for those who wish to propagate violent ideologies and influence audiences around the world in real time.[7] As Brynjar Lia, a research professor at the Norwegian Defence Research Establishment, noted, the Internet is "an important contributing factor in making terrorism more global and more transnational in scope" and assists in the creation and preservation of social bonds among leaders, supporters, and sympathizers.[8] Marc Sageman

"…the internet remains largely unregulated or un-mediated… stakeholders should not shy away from using it as yet another tool in the counterterrorism toolbox."

Liat Shetret is a programs officer at the Center on Global Counterterrorism Cooperation. The author wishes to thank her colleagues at the Center—Alistair Millar, James Cockayne, and Jason Ipe—for their valuable comments and critique. Thank you to Jack Barclay, independent consultant on strategic communications, for his insight, and feedback.

suggested that Internet communication serves as a "glue" to an otherwise "leaderless jihad."[9] Indeed, the Internet offers an ideal platform for media-minded terrorists to stimulate and supplement violent extremist activity off-line in the "real world." Terrorists acutely aware of these strengths are actively capitalizing on the advantages offered by online and off-line platforms.

The Internet can be exploited for terrorist purposes in numerous ways. It can be used for information gathering, fundraising, and data mining, as well as for reconnaissance purposes for potential attacks.[10] The Internet also is used to attract attention to a particular cause or grievance, to communicate and coordinate operations secretly, and to exchange instructive technical tradecraft manuals and guides.[11] In addition, the Internet is used to set agendas and disseminate repackaged information (or disinformation) as well as propaganda materials that draw on religious texts for legitimacy and validity. These materials are produced, authenticated, and distributed by affiliated media wings.[12]

The Internet also can be exploited as a communicative tool via Web sites, chatrooms, instant messaging, and social networking platforms to exchange ideas, share information, and strengthen a sense of community and personal identity, as well as reinforce a particular worldview or narrative. For example, over the past few years there has been an increase in the number of Web sites, podcasts, blogs, and social networking pages catering to al-Qaida's sympathizer community by calling for the use of violence.[13] These messages often are tailored to exploit vulnerable populations such as youth and linguistically are tailored specifically for Western audiences to encourage ideological buy-in.[14] It has been suggested that interactive forums and chatrooms are important, often critical "nodes" for communication, as they are difficult to monitor or remove, assure continuity of ideas and information flow, and facilitate interactive and dynamic discussions.[15]

Recruitment and radicalization are facilitated through strategic online communications and messaging consumed by local and global audiences. There remains considerable debate regarding to what extent activities on the Internet are complemented by physical relationships. Although most recruitment is believed to be rooted in off-line relationships and experiences in the real world, the Internet supplements and may replace traditional physical gathering spaces such as mosques, community centers, and coffee shops as recruitment venues.[16] Moreover, individuals' ability to self-select themselves in to specific Web sites or chatrooms hardens and reinforces particular worldviews and can facilitate the creation of an "alternative reality" and value systems.[17] Individuals continually choose to return to specific sources of information repeatedly. Over time, propaganda materials, videos, books, poetry, articles, music, and manuals assure potential recruits of the "righteousness of both the cause and the means adopted" and further legitimize and justify the use of violence.[18]

Challenges Facing Stakeholders Combating the Use of the Internet for Terrorist Purposes

Multilateral institutions, regional organizations, states, civil society, and other stakeholders have been grappling with the problem of the Internet being used to recruit and violently radicalize individuals across the globe.[19] Despite some important positive steps in this area, a number of challenges remain.

First, policies and programming have largely focused on technology-oriented approaches such as removing and banning Web sites.[20] It is important to distinguish between technological

and technical solutions to cybercrime (attacks on physical systems and infrastructure) and a social phenomenon such as communicative uses of the Internet described in this brief. Applying technological Band-Aids to social concerns naturally limits the positive and long-term impact banning and censoring mechanisms produce.[21] Although policing Web sites and content may be of some use, these mechanisms fail to counter the message itself as much of the narrative is not in fact illegal and does not call overtly for the use of violence.[22] Also, technological solutions applicable to our use of the Internet today, for example, to Web sites, chatrooms, and social networking platforms, may not apply to technological advances in the future and may be a waste of valuable resources. Also, censoring and removing information raise significant human rights and civil liberty concerns in practice.

Second, the body of literature remains underdeveloped on topics such as violent radicalization, deradicalization, and prevention, particularly operational, virtually based counterstrategies. Stakeholders are forced to address these challenges with limited data or empirically tested models.[23] Although the past few years have produced significant amounts of studies, long-term research and functional models—those that are applicable online in a variety of geographical, cultural, and linguistic circumstances—remain limited in scope.[24] Stakeholders will be empowered significantly by a drastic expansion of a virtually applicable knowledge base derived from strategies rooted in off-line empirical studies and research that is multilingual and cross-cultural.

Third, although there is growing awareness of what can be done to combat this problem on a social level, implementation remains uncoordinated, haphazard, and particularly challenging on issues of counternarratives.[25] According to the United States Institute of Peace, "Fragmented efforts of public diplomacy, strategic communications and information operations are underresourced, poorly coordinated, and understaffed given the strength and pervasiveness of [al-Qaida's] message."[26] Indeed, media-savvy terrorist organizations are good at what they do. Nimble media wings are capitalizing effectively on the Internet's advantages, while lumbering bureaucracies struggle to balance accountability and swift response and are structurally inflexible. Even though some stakeholders have managed to overcome organizational barriers, they continue to struggle with ways to identify and convince reliable messengers to deliver a counternarrative, particularly one that is locally relevant, inspiring, and germane to community concerns. Stakeholders especially are concerned about coming up with ways to transmit messages online credibly and effectively without being dismissed as tainted or untrustworthy.

States and other stakeholders are looking specifically for practical, financially feasible policy solutions to these issues. The UN Counter-Terrorism Implementation Task Force (CTITF), for example, has produced a report of the Working Group on Countering the Use of the Internet for Terrorist Purposes. The report presents a comprehensive "overview of approaches taken, primarily by Member States, towards countering use of the Internet for terrorist purposes."[27] A separate report of the cochairs of the CTITF Working Group on Radicalisation and Extremism That Lead to Terrorism conducted a mapping survey "with the objective of creating an inventory of counterradicalisation and deradicalisation measures implemented by Member States."[28] Some national strategies include entire network shutdowns, blacklisting, or banning of Web sites. States are actively employing counterradicalization, deradicalization, and counternarrative

"Equipping states with a real-world framework that aligns with civil liberties and human rights norms… will hopefully offer a fresh perspective on tackling an enormously complicated problem…"

programs as well as a wide variety of technical interceptive mechanisms.[29] Additionally, legislative actions, passive monitoring, and automated surveillance are being used as states attempt to identify, monitor, regulate, and minimize the influence of messaging rallying individuals toward the use of violence.[30]

It has been shown, however, that state-driven content reduction strategies are not only "crude, expensive and counterproductive," they are largely ineffective against interactive new media and social networking platforms such as Facebook and do not treat the "conversational" part of the problem.[31] Although some social networking programs and chat-enabled Web sites and forums can be banned entirely or monitored, it is financially, logistically, and legally problematic to track and disrupt millions of conversations on a global scale simply because they may promote or lead to violent radicalization.

Application of off-line radicalization process models may help to ensure that mechanisms and programs employed by stakeholders are rooted in empirical research and are affordable and effective in interrupting terrorist use of the Internet. Equipping states with a real-world framework that aligns with civil liberties and human rights norms and is applicable to the "ungoverned" cyberspace will hopefully offer a fresh perspective on tackling an enormously complicated problem and help break it down to smaller, manageable, policy-relevant elements.

Capitalizing on the Characteristics of the Internet for Counterterrorism Purposes

In September 2007, a senior member of al-Qaida presented a specific set of guidelines and strategic advice on how to exploit the weaknesses of al-Qaida to diminish its operational capabilities and ideological appeal and attraction.[32] In his video message, Abu Yahya al-Libi explicitly challenged the U.S. and other governments interested in countering the appeal of al-Qaida to "degrade the resonance of the jihadist message" and to turn the jihadist movement's own weaknesses against itself. Among other ideas, he specifically emphasized that no single government is able to implement a strategy to defeat the movement on its own and that ex-jihadists should be used, particularly in the Western media, to expose the weakness of al-Qaida's ideology and message of "anti-Muslim oppression and global jihad."[33] He advises his audience to amplify the voices of victims of terrorist activities, to emphasize the harming of "the innocent." He particularly emphasizes this strategy as a way to resonate with religious communities worldwide and therefore delegitimize the use of violence. Despite al-Libi's al-Qaida membership and affiliation, his strategic advice essentially aligns with what multiple stakeholders have been trying to implement and achieve in past years. The Internet can be used to implement some of these ideas effectively.

The Internet, where available, offers a systematic organization of the world's knowledge and facilitates the exposure of users to other cultures and ideas and altogether promotes a sense of "global community."[34] Main characteristics of the Internet include the creation of networks, anonymity of usage, and its self-selective, participatory, increasingly interactive nature. Although there are examples of censorship of the Internet by some countries, the Internet remains largely unregulated or unmediated and actually bypasses censorship mechanisms and reaches users directly via a personal computer or handheld device such as a mobile phone. These characteristics allow the platform to be used both for benign and illicit purposes, and stakeholders should not shy away from using it

as yet another tool in the counterterrorism toolbox.

In an attempt to better explain the involvement of individuals in politically motivated violence, experts and scholars have been developing research-based models describing potential pathways into, through, and out of terrorism.[35] Deductive insights from violent radicalization process models can be administered through the Internet in order to interrupt the communicative and instrumental uses of the Internet for terrorist purposes. The next section identifies four intervention opportunities that exemplify how concepts drawn from real-world models can help stakeholders effectively counter terrorism.

Opportunities for Intervention

Multilateral institutions, civil society organizations, the media, and the private sector all can draw on empirically based violent radicalization process models to intervene and effectively (1) weaken cult personalities, (2) challenge the extremist doctrine, (3) dispel the glory of the "terrorist lifestyle," and (4) offer a street-smart and locally developed and communicated counternarrative. These points are samples of roles and activities that may be taken by a variety of stakeholders and are mutually reinforcing and complementary. Across these four points, the importance of a credible messenger, one who is culturally and linguistically relevant and organic to a local community, cannot be overemphasized.

1. Weaken cult personalities

The counterterrorism community has been somewhat helpless in confronting so-called bridge figures—extremist ideologues, theorists, and scholars who are extremely charismatic, ambitious, and prolific and yet advocate the use of violence.[36] States have been very active in shutting down Web sites and forums, only to have them pop up under a new name and new server a little while later. Instead of shutting them down, damaging a personality's credibility and credentials as well as challenging their leadership role may be more effective in the long run.[37]

Technologically savvy individuals, such as al-Awlaki, have the ability initially to intrigue and over time to hook individuals into the narrative and movement. They have an active, timely, and well-developed Web presence that remains unchallenged and unrestricted. Al-Awlaki, for example, maintains an updated Web site and offers hundreds of videos and audio lectures online as well as bilingual written materials, attracting a broad and global audience. He also offers specifically tailored seminars to youth, women, and the impoverished and appeals to the masses.[38] The accessibility of materials via the Internet and simplicity of message has helped him establish a strong online support base and foundation of followers who find his leadership and message appealing and inspiring.[39]

The Internet can be used by stakeholders to discredit the legitimacy of these notorious experts and clerics. For example, stakeholders can draw on al-Libi's suggestion of anonymously circulating negative rumors and stories to damage the credibility and appeal of these cult personalities. In March 2010, for example, Shaykh-ul-Islam Dr. Muhammad Tahir-ul-Qadri issued a 600-page fatwa condemning terrorism.[40] The fatwa was presented in English and Urdu and was launched via international media outlets. That summer, ul-Qadri offered a summer antiterrorism camp program in the United Kingdom designed to offer youth alternative messaging regarding the role of spirituality, leadership and Islam in their lives.[41]

A point-by-point counternarrative and monitoring strategy can be developed further

"… amplify non-extremist voices from the grassroots through expanded yet targeted online content development & dissemination…"

to identify and elevate legitimate clerics and scholars who should remain free of government influence. Independence of the messenger is critical as it allows for civil society, the media, and other individuals through blogs or forums to organically oppose and challenge radically violent messaging without appearing to serve any political agenda. Governments often are perceived as being duplicitous and insincere in their attempts at counterradicalization, and perceived independence is crucial. For example, specialized Web sites, videos, and chat forums already in existence can be disseminated strategically to offer former terrorists, victims, celebrities, and businesspeople a broad platform for their message. Developing alternative, locally based cult personalities will offer competing information sources for figures such as al-Awlaki and challenge his support base with new ideas over time. Additionally, members of civil society, who are by definition active on the ground and in the online local circles (forums and Web sites), could serve as monitors or early-warning sirens once a rising-star personality calling for the use of violence appears on the virtual horizon.

2. Challenge the extremist doctrine

As mentioned above, the Internet often is used to spread and reinforce particular ideas, worldviews, and violently radical messages or narratives. Some narratives exploit the religion of Islam for inspiration and contain very specific messaging and repetitive themes that together shape and reinforce a narrow worldview and, in some cases, legitimize and justify the use of violence.[42]

Elements of a narrative endorsing the use of violence vary by the geographic location, societal vulnerability and susceptibility, language, culture, and education level of the targeted audience. Often, local or global grievances are linked to a particular narrative as a hook to elevate the organizational prestige and its global agenda and reach.[43] The Internet can be used to challenge specific dimensions of this narrative and offer content-tailored counterarguments for narratives endorsing and promoting the use of violence.

Alternative sources of information, such as respected individuals or organizations of civil society, can capitalize on the benefits of the Internet to expand their virtual presence and directly contradict violent messages and engage interlocutors online. It is important to amplify nonextremist voices from the grassroots through expanded yet targeted online content development and dissemination, increased access to the Internet by civil society groups, and use of graphic visuals and multimedia to support persuasive language.[44]

3. Dispel the glory of the "terrorist lifestyle"

Radical clerics and ideologues often glamorize and aggrandize the life of activists and martyrs and ignore the real-world lack of romance associated with this role. According to many narratives that endorse the use of violence, the daily emotional, psychological, and physical struggle of victims of terrorist attacks are rarely acknowledged and are significantly marginalized or attributed as collateral damage to the cause. Members of civil society are particularly well placed to pointedly contradict these notions. In these online communications, a special emphasis must be placed on highlighting the inglorious nature of a terrorist's life and daily separation from family and undisputedly denouncing the concept of martyrdom and use of violence for political ends.[45]

Online content development, in particular graphic, viral imagery and videos, could put a significant dent in any assertions linking honor, prestige, or glory with acts of violence.

The international community can offer support and technical assistance to civil society, investigative media sources, and the private sector or other stakeholders interested in expanding their advocacy and messaging on the Internet platform.

4. Offer a street-smart and locally developed and communicated counternarrative

A counternarrative, like the narrative it is trying to oppose, should offer a beginning, middle, and end and a purpose and be constructed as a social approach that educates and empowers communities.[46] It should specifically "appeal to those who are currently feeling alienated and marginalized."[47] A counternarrative must be geographically and culturally relevant and be based on the systematic collection and analysis of data and intelligence. Moreover, a counternarrative should establish or reestablish credibility and must be consistent with other actions taken by states, organizations, militaries, and legislatures and the foreign and domestic policies they promote.[48] There is little current focus on the potential role of a counternarrative in "promoting psychological disengagement."[49] "The effectiveness of any counter-narrative will rely heavily on the credibility and relevant expertise of the communicator."[50]

An online, street-smart counternarrative, one that draws on the Internet's strengths, ought to exploit the main characteristic of the Internet—its anonymity—and serve as a decentralized source of information. Government agencies, for example, can use the Internet to quietly unleash a flood of information that paints terrorist ideology in a negative light. As al-Libi advised the United States, "[G]overnments need to convince their populations that the murder of innocent people is a core part of global Jihadism."[51] One of the examples he provided in his video in 2007 was a rumor circulating about al-Qaida's constitution, suggesting that death is the penalty deemed for any al-Qaida retractors. This rumor, circulated online in chatrooms and forums, consequently will tarnish al-Qaida's image. In this example, the source of the rumor was irrelevant; in fact, the anonymity and reach of the Internet facilitated its effective spread.

Conclusion

Violent extremists are advocating on and off-line for the use of violence as a legitimate tool of struggle. This trend is on the rise. Of particular concern is the prevalence of these types of messages on the Internet in multiple languages. Stakeholders around the globe are concerned that these multilingual materials are contributing to the sympathizer and activist base of al-Qaida and its affiliates, perhaps even having a direct impact on the rise in individual lone wolves and homegrown terrorism around the globe.[52] Also, multimedia materials, visual illustrations, and texts glorifying the use of violence as a legitimate tactic of "struggle" are increasing in availability and quality and contributing to the establishment of the underdog status for which terrorist organizations aim. Of particular concern is a "slowly growing number of internet sites publishing documents on strategic thought, specifically war-fighting strategies," which can offer valuable insight to practitioners or pose a significant threat if ignored or underestimated.[53]

This brief has argued that real-world models of violent radicalization processes offer insight for policymakers in formulating points of intervention that are applicable in an online environment. Four brief points were made to demonstrate windows of interception by a variety of stakeholders. Many more should be explored and developed in depth and should draw in particular on existing and well-developed bodies of research such as network theory, cultural intelligence theory, cult theory,

and other social psychological constructs. All of these theories have been developed primarily to understand, prevent, and counteract off-line behaviors but should inspire additional research aimed at tackling not only off-line but also online behaviors.

Analysis often has focused on examples drawn from national experiences in the United Kingdom and its legal system and political conditions.

Although the body of literature is sprinkled with examples from Egypt, Indonesia, Jordan, Saudi Arabia, and the United States, the international community could benefit significantly by exploring other national experiences.

Over time, elements of virtual national models of counterviolent radicalization could be internationalized into a compilation of best practices that can be used as guidance and adapted to specific localized circumstances. Moreover, an effective method or program of tracking and evaluating in this field may be a useful research endeavor.

Additionally, existing efforts to counter cybercrime and eliminate so-called virtual safe havens should be examined to identify ways in which the same legislation or initiatives could be used to intercept instrumental and communicative aspects of the online platform mentioned in this brief. Assessing trends and formulating strategies that are more proactive than reactive may save resources in the long run.

An international commitment to a holistic counternarrative strategy should explore questions such as: What narrative are we looking to counter? Who is the messenger for this counternarrative work? What is the best medium to communicate a counternarrative? How does a counternarrative tactic fit into a broader scheme of online and off-line activities to counter radicalization?

Finally, it may be worth exploring how multilateral institutions, civil society organizations, the media, and the private sector can all draw on the Internet as a coordinative, harmonizing counterterrorism tool to prevent and counter the use of the Internet for terrorist purposes and to prevent duplication of activities and efforts.

The views expressed in this policy brief are those of the author and do not necessarily reflect those of the Center on Global Counterterrorism Cooperation, its staff, or advisory council.

Notes

[1] One example involves the December 2010 Stockholm bombings suspect Taimour Abdulwahab al-Abdaly, an Iraqi-born Swedish citizen who had an active Facebook profile and subscribed to a number of Google Groups. Investigators believe terrorists used addresses found online in an outdated directory of Chicago Jewish institutions to send package bombs on cargo airplanes from Yemen to the United States.

[2] Jack Barclay, "Challenging the Influence of Anwar al-Awlaki," *Developments in Radicalisation and Political Violence Series*, September 2010, http://icsr.info/publications/papers/1283965345ICSR_ChallengingtheInfluenceofAnwarAlAwlaki.pdf.

[3] Basil Katz, "Times Square Bomber Planned Second Attack," Reuters, 29 September 2010, http://www.reuters.com/article/idUSTRE68S50120100929.

[4] Ibid.

[5] Barclay, "Challenging the Influence of Anwar al-Awlaki."

[6] For examples of relevant models, see John Horgan, *Walking Away From Terrorism: Accounts of Disengagement From Radical and Extremist Movements* (London: Taylor and Francis, 2009) (Max Taylor and Horgan's seven-step nonlinear arc model); Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat," New York City Police Department, 2007, http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf (radicalization process model); Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008), pp. 71–88 (Four-Prong Theory); Sophia Moskalenko and Clark McCauley, "Measuring Political Mobilization: The Distinction Between Activism and Radicalism Intentions," *Terrorism and Political Violence* 21, no. 2 (2009): 239–260 (Activism and Radicalism Intention Scales [ARIS]).

[7] Sageman, *Leaderless Jihad*.

[8] Brynjar Lia, "Al Qaeda Online: Understanding Jihadist Internet Infrastructure," *Jane's Intelligence Review* 18, no. 1 (2006), http://www.mil.no/multimedia/archive/00075/Al-Qaeda_online__und_75416a.pdf.

[9] Marc Sageman, "A Strategy for Fighting International Islamist Terrorists," *ANNALS of the American Academy of Political and Social Science* 618, no. 1 (July 2008): 223–231.

[10] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C.: United States Institute of Peace, 2006).

[11] Anthony Bergin et al., "Countering Internet Radicalisation in Southeast Asia," *ASPI Special Report*, no. 22 (March 2009), http://www.aspi.org.au/publications/publication_details.aspx?ContentID=202 (hacking, firearms, and bomb-making manuals).

[12] Some examples are al-Fajar and the Global Islamic Media Front.

[13] Brynjar Lia, "Jihadi Web Media Production: Characteristics, Trends and Future Implications" (paper presented at "Monitoring, Research and Analysis of Jihadist Activities on the Internet: Ways to Deal With the Issue," Berlin, 26–27 February 2007), http://www.mil.no/multimedia/archive/00092/Jihadi_Web_Media_Pro_92100a.pdf.

[14] Center on Global Counterterrorism Cooperation, "Brainstorming on Youth Radicalization in the Mediterranean," 11–12 July 2007, http://www.globalct.org/images/content/pdf/discussion/rome_brainstorming.pdf (discussion paper).

[15] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

[16] Frank J. Cilluffo, testimony before the Senate Committee on Homeland Security and Governmental Affairs, 3 May 2007, p. 1, http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=00c59436-eb6e-46aa-8524-9073a57df152.

[17] Sageman, *Understanding Terror Networks*.

[18] Frank Cilluffo et al., "NETworked Radicalization: A Counter-Strategy," 2009, http://www.gwumc.edu/hspi/old/reports/NETworked%20Radicalization_A%20Counter%20Strategy.pdf.

[19] See Raphael F. Perl, "Terrorist Use of the Internet: Threats, Issues, and Options for International Co-operation" (remarks before the Second International Forum on Information Security, Garmisch-Partenkirchen, 7–10 April 2008), http://www.osce.org/documents/cio/2008/04/30594_en.pdf.

[20] See Tim Stevens and Peter R. Neumann, "Countering Online Radicalisation: A Strategy for Action," International Centre for the Study of Radicalisation and Political Violence, 28 January 2009, http://www.icsr.info/publications/papers/1236768491ICSROnlineRadicalisationReport.pdf.

[21] Weimann, *Terror on the Internet*.

[22] Jack Barclay, conversation with author, 13 December 2010.

[23] Sageman, *Understanding Terror Networks*.

[24] Weimann, *Terror on the Internet*. See Horgan, *Walking Away From Terrorism*.

[25] Col. John M. Venhaus, "Why Youth Join al-Qaeda," *United States Institute of Peace Special Report*, no. 236 (May 2010), http://www.usip.org/files/resources/SR236Venhaus.pdf; Weimann, *Terror on the Internet*.

[26] Venhaus, "Why Youth Join al-Qaeda."

[27] UN Counter-Terrorism Implementation Task Force (CTITF), "Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes," February 2009, http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf.

[28] Thirty-four member states out of 192 provided responses to the inventory request. CTITF, "First Report of the Working Group on Radicalisation and Extremism That Lead to Terrorism: Inventory of State Programmes," n.d., http://www.un.org/terrorism/pdfs/Report%20of%20the%20Working%20Group%20-%20Workgroup%202.pdf.

[29] CTITF, "Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes."

[30] U.S. Department of Justice, "The USA PATRIOT Act: Preserving Life and Liberty," n.d.,

http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf. Singapore monitors Internet use as an intimidation tactic and has monopolized Internet service throughout the state. Thailand monitors Internet café use and keeps track of users.

[31] Stevens and Neumann, "Countering Online Radicalisation." See Frank J. Cilluffo, Jeffrey B. Cozzens, and Magnus Ranstorp, "Foreign Fighters: Trends, Trajectories and Conflict Zones," George Washington University Homeland Security Policy Institute, 1 October 2010, http://www.gwumc.edu/hspi/policy/report_foreignfighters501.pdf.

[32] Jarret Brachman, "Abu Yahya's Six Easy Steps for Defeating al-Qaeda," *Perspectives on Terrorism* 1, no. 5 (April 2008), http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=18&Itemid=54.

[33] Venhaus, "Why Youth Join al-Qaeda."

[34] Bergin, "Countering Internet Radicalisation in Southeast Asia."

[35] A particularly useful and instructive model is Taylor and Horgan's seven-step nonlinear arc model. The violent radicalization process model captures an important distinction between two phases: ideological radicalization and violent radicalization. For further discussion, see Horgan, *Walking Away From Terrorism*.

[36] Cilluffo, Cozzens, and Ranstorp, "Foreign Fighters."

[37] Stevens and Neumann, "Countering Online Radicalisation."

[38] Barclay, "Challenging the Influence of Anwar al-Awlaki."

[39] Ibid.

[40] "Historical Launching of Fatwa Against Terrorism," Minhaj-ul-Quran International, 2 March 2010, http://www.minhaj.org/english/tid/9959/Historical-Launching-of-Fatwa-Against-Terrerism-leading-Islamic-authority-launches-fatwa-against-terrorism-and-denounces-suicide-bombers-as-disbelievers-Anti-terror-Fatwa-launched.htm.

[41] Henry Ridgewell, "Anti-Terrorism Summer Camp Held in Britain," Voice of America, 13 August 2010, http://www.voanews.com/english/news/europe/Anti-Terrorism-Summer-Camp-Held-In-Britain-100649109.html.

[42] Tom Quiggin, "Understanding al-Qaeda's Ideology for Counter-Narrative Work," *Perspectives on Terrorism* 3, no. 2 (August 2009): 18–24, http://www.terrorismanalysts.com/pt/articles/issues/PTv3i2.pdf.

[43] Anne Speckhard, "Contextual and Motivational Factors in the Pathways to Radicalization: Why Location Matters," in *Protecting the Homeland From International and Domestic Terrorism Threats: Current Multi-Disciplinary Perspectives on Root Causes, the Role of Ideology, and Programs for Counter-radicalization and Disengagement*, ed. Laurie Fenstermacher et al., January 2010, http://www.start.umd.edu/start/publications/U_Counter_Terrorism_White_Paper_Final_January_2010.pdf.

[44] Cilluffo et al., "NETworked Radicalization."

[45] Marc Jacobson, "Terrorist Drop-outs: One Way of Promoting a Counter-Narrative," *Perspectives on Terrorism* 3, no. 2 (August 2009), http://www.terrorismanalysts.com/pt/articles/issues/PTv3i2.pdf.

[46] Christian Leuprecht et al., "Narratives and Counter-Narratives for Global Jihad: Opinion Versus Action," in *Countering Extremist Narratives* (The Hague: National Coordinator for Counterterrorism, 2010), pp. 58–70, http://post.queensu.ca/~leuprech/docs/Leuprecht%20et%20al.-1.pdf. See Quiggin, "Understanding al-Qaeda's Ideology for Counter-Narrative Work."

[47] Cilluffo et al., "NETworked Radicalization."

[48] Deirdre Collings and Rafal Rohozinski, "Bullets and Blogs: New Media and the Warfighter," Center for Strategic Leadership, U.S. Army War College, October 2009, http://www.carlisle.army.mil/DIME/documents/Bullets__Blogs_new_Media__warfighter-Web(20%20Oct%2009).pdf.

[49] Horgan, *Walking Away From Terrorism*, p. 149.

[50] Ibid.

[51] Brachman, "Abu Yahya's Six Easy Steps for Defeating al-Qaeda."

[52] Lia, "Al Qaeda Online."

[53] Ibid.