Terrorist Use of the Internet: Information Operations in Cyberspace

Catherine A. Theohary
Analyst in National Security Policy and Information Operations

John Rollins
Specialist in Terrorism and National Security

March 8, 2011

Congressional Research Service
7-5700
www.crs.gov
R41674

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The Internet is used by international insurgents, jihadists, and terrorist organizations as a tool for radicalization and recruitment, a method of propaganda distribution, a means of communication, and ground for training. Although there are no known reported incidents of cyberattacks on critical infrastructure as acts of terror, this could potentially become a tactic in the future.

There are several methods for countering terrorist and insurgent information operations on the Internet. The federal government has organizations that conduct strategic communications, counterpropaganda, and public diplomacy activities. The National Framework for Strategic Communication guides how interagency components are to integrate their activities. However, these organizations may be stovepiped within agencies, and competing agendas may be at stake. This report does not discuss technical and Internet architecture design solutions.

Some may interpret the law to prevent federal agencies from conducting "propaganda" activities that may potentially reach domestic audiences. Others may wish to dismantle all websites that are seen to have malicious content or to facilitate acts of terror, while some may have a competing interest in keeping a site running and monitoring it for intelligence value.

Key issues for Congress:

- Although the Comprehensive National Cybersecurity Initiative addresses a federal cybersecurity strategy and departmental roles and responsibilities, overclassification, competing equities, and poor information sharing between agencies hinder implementation of a national cybersecurity strategy. (See "Federal Government Efforts to Address Cyberterrorism.")
- Federal agencies have interpreted the United States Information and Educational Exchange Act of 1948 (22 U.S.C. § 1461), also known as the Smith-Mundt Act, as creating a "firewall" between foreign and domestic audiences, limiting U.S. government counterpropaganda activities on the Internet. (See "Institutional Constraints.")
- Some agencies favor monitoring and surveillance of potentially harmful websites, while others would shut them down entirely. (See "Intelligence Gain/Loss Calculus.")
- Different agency approaches to combating terrorists' use of the Internet and different definitions and strategies for activities such as information operations (IO) and strategic communications (SC) create an oversight challenge for Congress. (See "Counterpropaganda: Strategic Communications, Public Diplomacy, and Information Operations.")

Cybersecurity proposals from the 111th Congress such as S. 3480, which contained controversial provisions labeled by the media as the Internet "Kill Switch," are likely to be reintroduced in some form in the 112th Congress. (See "Congressional Activity.") With growing interest in strategic communications and public diplomacy, there may also be an effort to revise the Smith-Mundt Act.

Contents

Background 1
Why and How International Terrorists Use the Internet 2
Propaganda, Recruitment, and Training 3
Cybercrime and Fund-Raising 4
Cyberattacks 5
Federal Government Efforts to Address Cyberterrorism 6
Federal Government Monitoring and Response 7
Counterpropaganda: Strategic Communications, Public Diplomacy, and Information Operations 8
Department of Defense Offensive Response 10
Federal Government Challenges and Implications 12
Institutional Constraints 12
Intelligence Gain/Loss Calculus 13
Congressional Activity 14

Contacts

Author Contact Information 16

Background

This report describes the ways that international terrorists and insurgents use the Internet, strategically and tactically, in pursuit of their political agendas.[1] This discussion covers terrorist information operations in cyberspace but does not discuss similar activities in other domains. The government response is also discussed in terms of information operations. Technical aspects of cybersecurity and network intrusion detection are outside the scope of this report.

Information warfare can be defined as the use of information technology and content to affect the cognition of an adversary or target audience. Information operations is defined by the Department of Defense as "the integrated employment ... of information-related capabilities in concert with other lines of operations to influence, corrupt, disrupt or usurp the decision-making of adversaries and potential adversaries while protecting our own."[2] One area where these operations can take place is cyberspace, defined by the Department of Defense as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers."[3] This report focuses on one particular element of the information environment: the Internet.

Terrorists make use of the Internet in a variety of ways, including what are often referred to as "jihadist websites." Most Al Qaeda-produced ideological material reflects Al Qaeda supporters' shared view of *jihad* as an individual duty to fight on behalf of Islam and Muslims, and, in some cases, to offensively attack Muslims or non-Muslims who are deemed insufficiently pious or who oppose enforcement of Islamic principles and religious law.[4] Al Qaeda and other violent Islamist

[1] Multiple definitions for "insurgency" and "terrorism" exist within the federal government. This report uses the Department of Defense doctrinal definition, which defines terrorism as "the calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological," and insurgency as "an organized resistance movement that uses subversion, sabotage, and armed conflict to achieve its aims. Insurgencies normally seek to overthrow the existing social order and reallocate power within the country."

[2] See Secretary of Defense Memorandum, Subject: Strategic Communication and Information Operations in the DoD, January 25, 2011. An earlier definition in Joint Publication 3/-13 defines IO as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."

[3] See Deputy Secretary of Defense Memorandum, Subject: The Definition of Cyberspace, May 12, 2008. The DOD finds this definition consistent with National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), which states that cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."

[4] The Arabic word *jihad* is derived from a verb that means "to struggle, strive, or exert oneself." Historically, key Sunni and Shia religious texts most often referred to jihad in terms of religiously approved fighting on behalf of Islam and Muslims. Some Muslims have emphasized nonviolent social and personal means of jihad or have sought to shape the modern meaning of the term to refer to fighting only under defensive circumstances. This report uses the term "jihad" to denote violent Sunni Islamists' understanding of the concept as a religious call to arms and uses the terms "jihadi" and "jihadist" to refer to groups and individuals whose statements indicate that they share such an understanding of jihad and who advocate or use violence against the United States or in support of transnational Islamist agendas. Alternative terms include "violent Islamist" or "militant Islamist." The term Islamist refers to groups and individuals who support a formal political role for Islam through the implementation of Islamic law by the state, political action through a religious party, or the creation of a religious system of governance. Islamists differ in their theological views and political priorities. For more information on Islam, jihadist ideology, and Al Qaeda and its affiliates, see CRS (continued...)

groups draw on the Quran and other Islamic religious texts and adapt historical events to current circumstances as a propaganda tactic. This approach is prominently displayed in jihadists' use of the Internet for recruiting and propaganda purposes.

Why and How International Terrorists Use the Internet

The Internet is used as a prime recruiting tool for insurgents.[5] Extremists use chat rooms, dedicated servers and websites, and social networking tools as propaganda machines, as a means of recruitment and organization, for training grounds, and for significant fund-raising through cybercrime. These websites and other Internet services may be run by international terrorist groups, transnational cybercrime organizations, or individual extremists. YouTube channels and Facebook pages of Taliban and Al Qaeda supporters may radicalize Western-based sympathizers, and also provide a means for communication between these "lone wolf" actors and larger organized networks of terrorists. The decentralized nature of the Internet as a medium and the associated difficulty in responding to emerging threats can match the franchised nature of terrorist organizations and operations.[6] It is unclear how great a role the Internet plays in coordinating the efforts of a single group or strategy.

Many Arabic-language websites are said to contain coded plans for new attacks. Some reportedly give advice on how to build and operate weapons and how to pass through border checkpoints.[7] Other news articles report that a younger generation of terrorists and extremists, such as those behind the July 2005 bombings in London, are learning new technical skills to help them avoid detection by various nations' law enforcement computer technology.[8]

Cybercrime has now surpassed international drug trafficking as a terrorist financing enterprise. Internet Ponzi schemes, identity theft, counterfeiting, and other types of computer fraud have been shown to yield high profits under a shroud of anonymity. According to press reports, Indonesian police officials believe the 2002 terrorist bombings in Bali were partially financed through online credit card fraud.[9] There may be some evidence that terrorist organizations seek the ability to use the Internet itself as a weapon in an attack against critical infrastructures.[10] Also,

(...continued)

Report RS21745, *Islam: Sunnis and Shiites*, by Christopher M. Blanchard; and CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*, coordinated by John Rollins.

[5] Deputy Assistant Secretary of Defense Garry Reid, in testimony before the Senate Armed Services Subcommittee on Emerging Threats and Capabilities, hearing on U.S. government efforts to counter violent extremism, March 10, 2010.

[6] For an explanation of how a terrorist group is transformed and applicable U.S. policy implications, see CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*, coordinated by John Rollins.

[7] Ibid.

[8] Michael Evans and Daniel McGrory, "Terrorists Trained in Western Methods Will Leave Few Clues," *London Times*, July 12, 2005, http://www.timesonline.co.uk/tol/news/uk/article543004.ece.

[9] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace," *Washington Post*, December 14, 2004, http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html.

[10] For more information on critical infrastructures, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.

links between terrorist organizations and cybercriminals may show a desire to hone a resident offensive cyber capability in addition to serving as a means of procuring funds.

To some observers, the term "cyberterrorism" is inappropriate, because a widespread cyberattack may simply produce annoyances, not terror, as would a bomb, or other chemical, biological, radiological, or nuclear explosive (CBRN) weapon. However, others believe that the effects of a widespread computer network attack would be unpredictable and might cause enough economic disruption, fear, and civilian deaths to qualify as terrorism. At least two views exist for defining the term cyberterrorism as traditionally understood:

- **Effects-based.** Cyberterrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals other than terrorists.
- **Intent-based.** Cyberterrorism exists when unlawful, politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.[11]

Propaganda, Recruitment, and Training

In a July 2005 letter to Abu Musab al-Zarqawi, the late leader of Al Qaeda operations in Iraq, senior Al Qaeda leader Ayman al-Zawahiri wrote, "We are in a battle, and more than half of this battle is taking place in the battlefield of the media."[12] Terrorist organizations exploit the Internet medium to raise awareness for their cause, to spread propaganda, and to inspire potential operatives across the globe. Websites operated by terrorist groups can contain graphic images of supposed successful terrorist attacks, lists and biographies of celebrated martyrs, and forums for discussing ideology and methodology.

The Quetta Shura Taliban reportedly maintains several dedicated websites, including one with an Arabic-language online magazine, and publishes daily electronic press releases on other Arabic-language jihadist forums. The As-Shahab Institute for Media Production is Al Qaeda Central's media arm and distributes audio, video, and graphics products online through jihadist forums, blogs, and file-hosting websites.

A recent online English-language terrorist propaganda periodical called *Inspire* appears to have originated from the media arm of a Yemen-based Al Qaeda group and contains articles by Anwar al-Awlaki, an English-speaking, U.S.-born radical imam whose sermonizing rhetoric and calls to action make extensive use of cyberspace. Al-Awlaki has been connected to several terrorist plots, including the attempted Times Square bombing in New York City in May 2010. Al-Awlaki has also been either directly or indirectly linked to radicalizing Nidal M. Hasan, who allegedly committed the November 2009 shooting at Fort Hood, Texas, and Umar Farouk Abdulmutallab, the Nigerian suspect accused of trying to ignite explosives on Northwest/Delta Airlines Flight 253 on Christmas Day 2009. Faisal Shahzad, a naturalized U.S. citizen from Pakistan, admitted to

[11] For a more in-depth discussion of the definition of cyberterrorism, see CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John Rollins and Clay Wilson.

[12] A copy of the letter was released by the Office of the Director of National Intelligence on October 11, 2005, and can be accessed at http://www.globalsecurity.org/security/library/report/2005/zawahiri-zarqawi-letter_9jul2005.htm.

trying to set off a car bomb in Times Square and said he was inspired by al-Awlaki's online lectures.

Some experts question the authenticity of the periodical *Inspire* and its link to Al Qaeda.[13] The effectiveness of violent images used to reach its mainstream target audience is debated, as the violent images may appeal only to a small, self-selected segment of the population. In the July 2005 letter discussed above, al-Zawahiri, in a reference to winning the "hearts and minds" of Muslims, noted that "the Muslim populace who love and support you will never find palatable ... the scenes of slaughtering the hostages."[14]

These websites can also carry step-by-step instructions on how to build and detonate weapons, including cyber weapons. One website reportedly carries a downloadable "e-jihad" application, through which a user can choose an Internet target and launch a low-level cyberattack, overwhelming the targeted website with traffic in order to deny its service. The websites may also contain instructions for building kinetic weapons, such as bombs and improvised explosive devices, as well as for conducting surveillance and target acquisition.[15]

The Internet can also be used to transmit information and material support for planned acts of terrorism. A recent case involving a U.S. citizen residing in Pennsylvania alleges that a woman using the nickname "JihadJane" posted messages on YouTube and used jihadist websites and chat rooms to plan and facilitate an overseas attack.[16]

Cybercrime and Fund-Raising

Cybercrime has increased in past years, and several recent terrorist events appear to have been funded partially through online credit card fraud. Extremist hackers have reportedly used identity theft and credit card fraud to support terrorist activities by Al Qaeda cells.[17] When terrorist groups do not have the internal technical capability, they may hire organized crime syndicates and cybercriminals through underground digital chat rooms. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists' desire to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

[13] One example is Max Fisher, in "Five Reasons to Doubt Al-Qaeda Magazine's Authenticity," *The Atlantic*, July 1, 2010, accessed at http://www.theatlantic.com/international/archive/2010/07/5-reasons-to-doubt-al-qaeda-magazines-authenticity/59035/.

[14] Ibid.

[15] For example, the online magazine *Inspire* contains an article entitled, "How to make a bomb in the kitchen of your Mom."

[16] Carrie Johnson, "JihadJane, an American woman, faces terrorism charges," *Washington Post*, March 10, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/09/AR2010030902670.html.

[17] According to FBI officials in a report issued in June 2005, Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases. Also, the FBI has recorded more than 9.3 million Americans as victims of identity theft in a 12-month period. Report by the Democratic Staff of the House Homeland Security Committee, *Identity Theft and Terrorism*, July 1, 2005, p. 10.

Cyberattacks

Although terrorists have been adept at spreading propaganda and attack instructions on the web, it appears that their capacity for offensive computer network operations may be limited. The Federal Bureau of Investigation (FBI) reports that cyberattacks attributed to terrorists have largely been limited to unsophisticated efforts such as e-mail bombing of ideological foes, denial-of-service attacks, or defacing of websites. However, it says, their increasing technical competency is resulting in an emerging capability for network-based attacks. The FBI has predicted that terrorists will either develop or hire hackers for the purpose of complementing large conventional attacks with cyberattacks.[18] During his testimony regarding the 2007 Annual Threat Assessment, FBI Director Robert Mueller observed that "terrorists increasingly use the Internet to communicate, conduct operational planning, proselytize, recruit, train and to obtain logistical and financial support. That is a growing and increasing concern for us."[19] In addition, continuing publicity about Internet computer security vulnerabilities may encourage terrorists' interest in attempting a possible computer network attack, or cyberattack, against U.S. critical infrastructure.

The Internet, whether accessed by a desktop computer or by the many available handheld devices, is the medium through which a cyberattack would be delivered. However, for a targeted attack[20] to be successful, the attackers usually require that the network itself remain more or less intact, unless the attackers assess that the perceived gains from shutting down the network entirely would offset the accompanying loss of their own communication. A future targeted cyberattack could be effective if directed against a portion of the U.S. critical infrastructure, and if timed to amplify the effects of a simultaneous conventional physical or chemical, biological, radiological, or nuclear (CBRN) terrorist attack. The objectives of a cyberattack may include the following four areas:

- loss of integrity, such that information could be modified improperly;
- loss of availability, where mission-critical information systems are rendered unavailable to authorized users;
- loss of confidentiality, where critical information is disclosed to unauthorized users; and
- physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.

Publicity would also potentially be one of the primary objectives for a terrorist cyberattack. Extensive media coverage has shown the vulnerability of the U.S. information infrastructure and the potential harm that could be caused by a cyberattack. This might lead terrorists to believe that even a marginally successful cyberattack directed at the United States would garner considerable publicity. Some suggest that were such a cyberattack by an international terrorist organization to occur and become known to the general public, regardless of the level of success of the attack,

[18] Statement of Steven Chabinsky, Deputy Assistant Director, FBI Cyber Division, before the Senate Judiciary Committee Subcommittee on Homeland Security and Terrorism, at a hearing entitled, *Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy Rights in Cyberspace*, November 17, 2009.

[19] Robert Mueller, FBI Director, testimony before the Senate Select Committee on Intelligence, January 11, 2007.

[20] A targeted attack is one where the attacker is intentionally attempting to gain access to or to disrupt a specific target. This is in contrast to a random attack, where the attacker seeks access to or to disrupt any target that appears vulnerable.

concern by many citizens and cascading effects might lead to widespread disruption of critical infrastructures. For example, reports of an attack on the international financial system's networks could create a fiscal panic in the public that could lead to economic damage.

According to security experts, terrorist groups have not yet used their own computer hackers nor hired hackers to damage, disrupt, or destroy critical infrastructure systems. Yet reports of a recent disruptive computer worm that has spread through some government networks, including that of the National Aeronautics and Space Administration, have found a possible link to a Libyan hacker with the handle "Iraq Resistance" and his online hacker group "Brigades of Tariq ibn Ziyad," whose stated goal is "to penetrate U.S. agencies belonging to the U.S. Army."[21] According to these reports, references to both the hacker and group have been found in the worm's code. However, this does not provide conclusive evidence of involvement, as e-mail addresses can be spoofed and code can be deliberately designed to implicate a target while concealing the true identity of the perpetrator.

The recent emergence of the Stuxnet worm may have implications for what potential future cyberattacks might look like. Stuxnet is thought to be the first piece of malicious software (malware) that was specifically designed to target the computer-networked industrial control systems that control utilities, in this case nuclear power plants in Iran. Although many experts contend that the level of sophistication, intelligence, and access required to develop Stuxnet all point to nation states, not only is the idea now in the public sphere for others to build upon, but the code has been released as well. An industrious group could potentially use this code as a foundation for developing a capability intended to degrade and destroy the software systems that control the U.S. power grid, to name one example.[22]

Federal Government Efforts to Address Cyberterrorism

A number of U.S. government organizations appear to monitor terrorist websites and conduct a variety of activities aimed at countering them. Given the sensitivity of federal government programs responsible for monitoring and infiltrating websites suspected of supporting terrorism-related activities, much of the information regarding the organizations and their specific activities is deemed classified or law enforcement-sensitive and is not publicly available. The information listed below represents a sampling of what has been publicly discussed about some of the federal government organizations responsible for monitoring and infiltrating jihadist websites. It should be noted that the actions associated with the organizations listed below could be conducted by employees of the federal government or by civilian contract personnel.

- Central Intelligence Agency (CIA): development, surveillance, and analysis of websites, commonly referred to as honey pots, for purposes of attracting existing and potential jihadists searching for forums to discuss terrorism-related activities.[23]

[21] See http://www.computerworld.com/s/article/9184718/Cyber_jihad_group_linked_to_Here_you_have_worm.

[22] For more information, see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John Rollins, and Catherine A. Theohary.

[23] Ellen Nakashima, "Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies," *Washington* (continued...)

- National Security Agency (NSA): surveillance of websites and rendering them inaccessible.[24]
- Department of Defense (DOD): surveillance of websites focused on discussions of perceived vulnerabilities of overseas U.S. military facilities or operational capabilities and disabling those that present a threat to operations.[25]
- Department of Justice (DOJ): development of polices and guidelines for creating, interacting within, surveilling, and rendering inaccessible websites created by individuals wishing to use the Internet as a forum for inciting or planning terrorism-related activities.
- Federal Bureau of Investigation (FBI): monitoring of websites and analysis of information for purposes of determining possible terrorist plans and threats to U.S. security interests.[26]
- Department of Homeland Security (DHS): monitoring of websites and analysis of information for purposes of determining possible threats to the homeland.[27]

Numerous other federal government organizations have cybersecurity responsibilities focused on policy development, public awareness campaigns, and intergovernmental and private sector coordination efforts. Information gleaned from the agencies noted above may at times be used to help inform and advise non-federal government entities responsible for safeguarding a geographic area or activity that has been discussed in an online jihadist forum.

Federal Government Monitoring and Response

A number of reasons exist that may provide justification for the federal government to monitor websites owned, operated, or frequented by individuals suspected of supporting international jihadist activity that pose a threat to U.S. security interests. Such websites may be used for purposes of spreading propaganda, recruiting new members or enticing existing participants, communicating plans counter to U.S. interests, or facilitating terrorist-related activities.[28] Quite often the jihadist websites are the first indicators of extreme elements of the jihadist community identifying a controversial issue for purposes of inciting action harmful to U.S. interests. For example, a recent controversy in the United States about a proposed burning of copies of the

(...continued)

Post, March 19, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html.

[24] Ibid.

[25] Ibid.

[26] Testimony of Steven Chabinsky, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security, "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace," November 17, 2009, http://www.fbi.gov/congress/congress09/chabinsky111709.htm.

[27] DHS, Privacy Impact Assessment for the Office of Operations Coordination and Planning, "2010 Winter Olympics Social Media Event Monitoring Initiative," February 10, 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_2010winterolympics.pdf.

[28] For additional information regarding terrorists use of the Internet, see Council of Foreign Relations backgrounder, *Terrorists and the Internet*, Eben Kaplan, January 8, 2009, http://www.cfr.org/publication/10005/terrorists_and_the_internet.html#p8.

Quran on the ninth anniversary of the September 11, 2001, attacks led to increased chatter[29] on international jihadist websites. The FBI reportedly disseminated an intelligence bulletin specifically noting online threats to the pastor and church planning to conduct this event and more general threats to U.S. global interests.[30]

When assessing whether to monitor, infiltrate, or shut down a website suspected of inciting participants to take harmful actions against U.S. security interests, numerous competing interests should be considered. First, the federal government would determine whether the website is owned by a U.S. corporation and whether U.S. citizens may be participating in the Internet forum. Such a determination is necessary to ensure that proper procedures are adhered to with respect to upholding the rights afforded by the U.S. Constitution's First and Fourth Amendments, in particular.[31] Second, once it is confirmed that a suspected jihadist website is being used to facilitate terrorism-related activities, the national security community may consider the short- and long-term implications of a variety of operational responses. Options include permanently or temporarily shutting down the website, passively monitoring the website for intelligence-gathering purposes, or covertly engaging the members of the forum with the desire to elicit additional information for purposes of thwarting a potential terrorism-related activity and/or building a stronger criminal case. Different agencies may weigh each option differently, creating a need to achieve interagency consensus prior to action.

DOD has been considering establishing a computer network monitoring database for government and private networks. Organizations would provide information on a voluntary basis, and the data collected would be shared with all participants. However, privacy concerns and questions of DOD's proper role in federal cybersecurity make the implementation of such a program unlikely in the current political climate. A memorandum of agreement signed in October 2010 between DHS and DOD represents an effort to increase coordination of operations and plans to protect civilian critical infrastructure as well as military networks.[32] The partnership could be used as a means through which DOD would have a greater role in defending privately owned critical infrastructure using the EINSTEIN 2 and 3 network monitoring systems developed by DHS.[33]

Counterpropaganda: Strategic Communications, Public Diplomacy, and Information Operations

In common parlance and in media reporting, the terms "strategic communications," "public diplomacy," "global engagement," "information operations," and "propaganda" are often used interchangeably. This confusion in terms makes it difficult to determine exactly what sorts of programmatic activities are being discussed. There is no overarching definition of strategic

[29] In Internet parlance, this term is used to describe the dialogue that takes place in chat rooms and other online discussion groups.

[30] Elaine Reyes, "FBI Issues Intelligence Bulletin Before Quran Burning," *MSNBC.Com*, September 9, 2010, http://www.msnbc.msn.com/id/39077427/.

[31] Address by Department of Homeland Security Secretary Janet Napolitano before the American Constitution Society for Law and Policy, 2010 American Constitution Society National Convention, June 18, 2010, http://www.acslaw.org/node/16377.

[32] This cybersecurity memorandum can be accessed at http://www.defense.gov/news/d20101013moa.pdf.

[33] The EINSTEIN program develops automated technology to detect and possibly prevent computer network intrusion. For more information, see the *Privacy Impact Assessment for the Initiative Three Exercise*, Department of Homeland Security, March 18, 2010.

communications for the federal government. DOD has defined strategic communication as "focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power."[34] This term, as defined, describes a U.S. government-wide process, not an organizational structure, capability, or discrete activity within DOD or any other government agency.

As prescribed by the 2009 National Framework for Strategic Communication, the Deputy National Security Advisor for Strategic Communications (DNSA/SC) serves as the National Security Advisor's principal advisor for strategic communications. The Senior Director for Global Engagement (SDGE) is the principal deputy to the DNSA/SC. Together, they are responsible for ensuring that (1) the message-value and communicative impact of actions are considered during decision-making by the National Security Council (NSC) and Homeland Security Council (HSC); (2) the mechanisms to promote strategic communication are in place within the National Security Staff (NSS); ,and (3) similar mechanisms are developed across the interagency. The DNSA/SC and SDGE are also responsible for guiding and coordinating interagency deliberate communication and engagement efforts, and they execute this responsibility through the NSS Directorate for Global Engagement (NSS/GE) and through the Interagency Policy Committee (IPC) on Strategic Communication.

Public Diplomacy (PD) within the State Department is led by the Under Secretary for Public Diplomacy and Public Affairs. The Department of State distinguishes between Public Affairs (PA), which includes outreach to domestic publics, and PD—which seeks to promote the national interest of the United States through understanding, engaging, informing, and influencing foreign publics, and by promoting mutual understanding between the people of the United States and people from other nations around the world.

In DOD, strategic communication-related activities are primarily supported by the integration of three capabilities: Information Operations (IO), and, primarily within IO, Psychological Operations (PSYOP),[35] Public Affairs (PA), and Defense Support to Public Diplomacy (DSPD). Military Diplomacy (MD) and Visual Information (VI) also support strategic communications-related activities. DOD sees strategic communications as a process to synchronize efforts that:

- improve U.S. credibility and legitimacy;
- weaken an adversary's credibility and legitimacy;
- convince selected audiences to take specific actions that support U.S. or international objectives;
- cause a competitor or adversary to take (or refrain from taking) specific actions.

[34] 2006 QDR Strategic Communication Execution Roadmap, accessed at http://www.defense.gov/pubs/pdfs/QDRRoadmap20060925a.pdf.

[35] Although influence operations are still frequently referred to as "psychological operations," the technical name for these activities has now been changed to Military Information Support Operations (MISO). See the "Institutional Constraints" section of this report for explanation.

Many DOD activities support the State Department's public diplomacy efforts and objectives, which in turn support national objectives. DOD refers to these activities as "Defense Support to Public Diplomacy" (DSPD).

Although some reports warn of social media's potential misuse by terrorists, government policies are evolving to embrace the use of tools such as Facebook and Twitter as a means of strategic communications and public diplomacy. On the one hand, according to a U.S. Army report, social media tools such as Twitter and Facebook can be used by terrorist groups to expand networks and exchange real-time information, enabling operatives to organize and act quickly.[36] These tools can not only spread propaganda, but can also host embedded malicious software in links and applications that can corrupt an unsuspecting user's electronic device. Based on these security concerns, several services and offices within DOD had banned certain social networking sites from access on their unclassified networks. However, the federal government has begun to embrace using these same tools to allow free access to information, spread democratic values and ideas, and combat the misinformation spread by terrorist groups' media campaigns. In February 2010, DOD issued a directive-type memo (DTM) outlining the department's new social media policy, citing Internet-based capabilities including social networking services as integral to operations.[37] This policy is due to expire in March 2011; reportedly, there are no plans to develop a replacement policy, nor plans to fill the top positions that were instrumental in creating the social media policy. Some fear that the recent WikiLeaks issue may push the pendulum back toward more restricted access to Internet-based capabilities and less information sharing between organizations. Others note that, to date, much of the activity conducted under the current policy has been one-sided, focused on using social network tools to gather information about others, including potential adversaries, rather than to send messages outward in order to shape the information environment. Reportedly, the U.S. Air Force and U.S. Central Command have been developing deceptive identities on the Internet in order to infiltrate chat rooms and other social media using a special software.[38] The U.S. Air Force software contract states that it shall be used to target adversarial sites worldwide without detection, and spokesmen for the U.S. Central Command have stated that it shall not be used to target law-abiding American citizens.[39] Critics of these programs point to the potential loss of credibility, a tenet of successful information operations, using the former Office of Strategic Influence (OSI) as an example. Reports that the OSI was planting false news stories into foreign newspapers to gain support for the war in Iraq led many—including the Public Affairs Office—to question the legality of such activity. The OSI was subsequently disestablished.

Department of Defense Offensive Response

Information operations do not refer exclusively to messaging and content; another integrated capability within this area is computer network operations (CNO), which includes cyberattack

[36] The report, presented by the 304th Military Intelligence Battalion, can be accessed through the Federation of American Scientists website at http://www.fas.org/irp/eprint/mobile.pdf.

[37] Office of the Deputy Secretary of Defense, Directive-Type Memorandum 09-026, *Responsible and Effective Use of Internet-Based Capabilities*, February 25, 2010.

[38] See Alison Diana, "Air Force Seeks Fake Online Social Media Identities," *Information Week*, February 22, 2011; and Shaun Waterman, "U.S. Central Command 'friending' the enemy in psychological war," *Washington Times*, March 1, 2011.

[39] U.S. Air Force Persona Management Software Solicitation Number: RTB220610, accessed at http://media.washingtonpost.com/wp-srv/politics/documents/personalsoftware0302.pdf.

capabilities, cyber espionage and exploitation, and cyber defense. The Joint Functional Command Component—Network Warfare (JFCC-NW) and the JFCC—Space & Global Strike (JFCC-SGS) have responsibility for overall DOD cybersecurity, while the Joint Task Force—Global Network Operations (JTF-GNO) and the Joint Information Operations Warfare Center (JIOWC) both have direct responsibility for defense against cyberattack.[40] The DOD focal point for coordinating military information operations is the JIOWC. The JTF-GNO defends the DOD Global Information Grid, while the JIOWC assists combatant commands with an integrated approach to information operations. These include operations security, military information support operations (formerly psychological operations), military deception, and electronic warfare. Many of the specific programs under the JIOWC's purview are classified. The JIOWC also coordinates computer network operations and network warfare with the JTF-GNO and with JFCC-NW. These latter two organizational activities are to fall under the responsibility of the newly formed U.S. Cyber Command (USCYBERCOM), a sub-unified command under U.S. Strategic Command (USSTRATCOM). The commander of USCYBERCOM, General Keith Alexander, also serves as the director of NSA. Traditionally, the NSA mission has been information assurance for national security systems and signals intelligence, and gathering information about potential threats under the Foreign Intelligence Surveillance Act (FISA). The dual-hatted nature of this appointment places this intelligence function alongside the offensive operations command.

Information security and cyberwarfare planners in the Pentagon have noted both in doctrine and in informal channels that a good offensive cyber operations capability is the best defense. For this reason, USCYBERCOM has integrated the military's defensive computer network operations components with its offensive arm under one joint command. Many of USCYBERCOM's capabilities are unknown, due to the classified nature of offensive cyber operations. There have also been questions in the executive branch and in Congress about what authorities they operate under and how oversight is to be conducted. A question-and-answer exchange from the Senate Armed Services Committee revealed that DOD had not included cyber operations in its quarterly report on clandestine military activities. Michael Vickers, the nominee for Undersecretary of Defense for Intelligence, reportedly told the committee that those quarterly reporting requirements related only to human intelligence. How USCYBERCOM relates to NSA and how both relate to the private sector, which owns most of the U.S. telecommunications infrastructure, has been a continued subject of discussions.

On the defensive side, although USCYBERCOM is developing plans to defend the .mil domain, there is still no unified federal response policy for coordinating offensive cyber operations at the national level. Yet DOD has been working with DHS and the National Cybersecurity and Communications Integration Center through Cyberstorm and other exercises to map out a National Cyber Incident Response Plan, which gives a structure for how the federal government might respond in the event of a major cyberattack. At a Reserve Officers Association conference, USCYBERCOM Chief of Staff Major General David Senty said that the sub-unified command might take the lead in defending the nation's military networks as a "supported command" prior to "turning things over" to U.S. Northern Command.[41]

[40] Clark A. Murdock et al., *Beyond Goldwater-Nichols: U.S. Government and Defense Reform for a New Strategic Era*, Phase 2 Report, July 2005, Center for Strategic and International Studies, p. 128, http://www.ndu.edu/lIbrary/docs/BeyondGoldwaterNicholsPhase2Report.pdf.

[41] A "supported command" is one that is operationally augmented by a subordinate component.

Federal Government Challenges and Implications

Although organizations, policies, and plans exist to counter violent extremists' use of the Internet, implementation may be hampered by several factors. Laws may be interpreted by some agencies to prohibit certain activities, and in some cases agencies may have competing equities at stake. Legislative and policy authority may be given to organizations that lack the technical capability to fulfill a mission, while entities with the capacity to address cyber attacks may be legally constrained from doing so due to privacy or civil liberties concerns. There may be tensions between the Global Internet Freedom Initiative as highlighted by Secretary of State Hillary Clinton and overall counterterrorism objectives. Additionally, the lack of clarity in definitions related to information operations and terrorism may lead to institutional questions such as which agency has the lead for federal government coordination or independent oversight.

Institutional Constraints

Some argue that the effectiveness of the U.S. government's strategic communications, information operations, and global engagement programs is still hampered by the U.S. Information and Educational Exchange Act of 1948 (22 U.S.C. § 1461), also known as the Smith-Mundt Act. The law directs that information about the United States and its policies intended for foreign audiences "shall not be disseminated within the United States, its territories, or possessions." Amendments to the Smith-Mundt Act in 1972 and 1998 further clarified the legal obligations of the government's public diplomacy apparatus, and several presidential directives, including NSPD-16 in July 2002, have set up specific structures and procedures as well as further legal restrictions regarding U.S. public diplomacy and information operations. Some say that these policies have created an unnecessary "firewall" between domestic and foreign audiences, limiting what information the United States produces and distributes to counter extremists in cyberspace for fear of "blow-back" to its own citizens. Cyberspace as a global domain does not recognize territorial boundaries, making it difficult to target a specific geographic region. Some argue that this has effectively created a ban on all government "propaganda," a term that carries with it negative historical connotations, although the term is neither defined nor mentioned in the law itself. Some critics argue that the law does not prevent government propagandizing, but rather has been consistently misinterpreted. Others maintain that the Smith-Mundt provisions may prevent undue government manipulation of citizens and are a necessary protection.

In addition to questions over what constitutes propaganda and the applicability of Smith-Mundt, confusion over "information operations" programs has led some to question their budgetary process and management within DOD. Often confused with Information Operations as a whole, PSYOP refers to influence activities specifically intended "to induce or reinforce foreign attitudes and behavior in a manner favorable to U.S. objectives." While PSYOP is focused at audiences abroad, it is supported by the public affairs function. The Public Affairs Office (PAO) is the entity responsible for working with media outlets both domestic and foreign, to "inform" rather than to "influence." Given the public's and government's aversion to the term "propaganda" and particularly military activities that might be described as such, DOD has changed military lexicon from PSYOP to Military Information Support Operations (MISO). The Secretary of Defense approved the name change in June 2010 following a recommendation from the Defense Senior Leadership Council. Some argue that the name change elevates the importance of information support to military operations for commanders in the field, while others point to the traditional career field of PSYOP as a source of pride among its servicemembers.

A January 2011 memorandum issued by DOD acknowledges the heightened strategic emphasis on countering violent extremism and transnational, global networks through effective strategic communications and information operations.[42] The memo outlines organizational changes that are designed to facilitate better program integration and coordination to meet these challenges. The new construct places the JIOWC under the Joint Staff in all but its electronic warfare coordinating function, which shall still remain the purview of USSTRATCOM. The memo also describes new requirements for resource managers to capture the costs of MISO and to develop standardized budget methodologies for SC and IO capabilities and activities. This is in response to congressional concerns over what constitutes an "information operation" and how much federal money is spent on what has been perceived as military propaganda.

The Department of Defense Appropriations Acts for FY2002 through FY2010 provide that, "No part of any appropriation contained in this Act shall be used for publicity or propaganda purposes not authorized by the Congress."[43] Title 10 of the *United States Code*, Section 167, authorizes combatant commanders to conduct psychological operations as part of clandestine special operations campaigns in support of military missions. However, Title 10 does not define PSYOP, nor does it clarify DOD's authority to conduct information operations versus propaganda.

Some private U.S. citizens have attempted to work outside of these institutional constraints. For instance, inspired by 9/11, Montana resident Shannen Rossmiller has been using the Internet to glean information about potential terrorist suspects and their plans. This information, which she has shared with federal intelligence agencies, has led to the arrests of a Washington state National Guardsman, convicted in 2004 of attempted espionage for plans to transmit U.S. military armor information through the Internet, and a Pennsylvania man who prosecutors say sought to blow up oil installations in the United States. As a self-taught private citizen, Ms. Rossmiller can operate outside of the institutional constraints that may bind federal employees. Rita Katz of Search for International Terrorist Entities (SITE Institute) performs similar activities, funneling intelligence mined from online extremist chat rooms to government officials without having to go through the sometimes onerous and time-consuming official channels. The intelligence agencies have not discussed publicly the nature of the information shared, nor how it was used.[44]

Intelligence Gain/Loss Calculus

Tensions between a website's purported intelligence value and operational threat level can determine the particular capabilities used to thwart the site. For example, a "honey pot" jihadist website reportedly was designed by the CIA and Saudi Arabian government to attract and monitor terrorist activities. The information collected from the site was used by intelligence analysts to track the operational plans of jihadists, leading to arrests before the planned attacks could be executed. However, the website also was reportedly being used to transmit operational plans for jihadists entering Iraq to conduct attacks on U.S. troops. Debates between representatives of the NSA, CIA, DOD, DNI, and NSC led to a determination that the threat to troops in theater was greater than the intelligence value gained from monitoring the website, and a computer network team from the JTF-GNO ultimately dismantled it. This case raised questions of whether computer

[42] Secretary of Defense Robert Gates, Memorandum for the Secretaries of the Military Departments, Subject: Strategic Communications and Information Operations in the DoD, January 25, 2011.

[43] This clause is known as a "propaganda rider," and was also in the Omnibus Appropriations Act of 2009, Title V, Section 501.

[44] See Blaine Harden, "In Montana, Casting a Web for Terrorists," *Washington Post*, June 4, 2006.

network attacks on a website are a covert operation or a traditional military activity, and under what authority they are conducted. It also illustrated the risk of collateral damage that an interconnected, networked world represents, as the operation to target and dismantle the honey pot inadvertently disrupted servers in Saudi Arabia, Germany, and Texas. Also, some point to the potential futility of offensively attacking websites, as a dismantled site may be easily relocated to another server.

The 2010 National Security Strategy mentions the importance of the Internet for commerce and for disseminating information, and the importance of cybersecurity in protecting national security assets, but does not appear to present a strategy specifically for combating violent extremism on the Internet.[45]

Congressional Activity

A number of hearings have been held to address the issue of violent extremism on the Internet.[46] In a March 2, 2010, "Dear Colleague" letter, members of the House of Representatives announced the formation of a new Strategic Communications and Public Diplomacy Caucus, whose stated purpose is to "raise awareness of the challenges facing strategic communication and public diplomacy and provide multiple perspectives on proposed solutions."[47] On July 13, 2010, the caucus's chairs, Representatives Mac Thornberry and Adam Smith, introduced H.R. 5729, the Smith-Mundt Modernization Act of 2010. This measure would amend the United States Information and Educational Exchange Act of 1948 to allow the Secretary of State to create products designed to influence audiences abroad that could also be disseminated domestically, thereby removing the "firewall."

Another piece of legislation introduced in the 111th Congress was S. 3480, the Protection of Cyberspace as a National Asset Act. This bill, which may be reintroduced in some form in the current Congress, has generated much discussion over what some describe as the "Internet Kill Switch." Recent events of social unrest and government Internet control in the Middle East highlight the question of whether the President has the authority to "turn off" the U.S. connection to the Internet in times of similar crisis and whether such authority is needed. Critics consider such a communication disruption as an attack on the freedom of speech and the free flow of information. Others point to the economic damage that could result from the loss of networked communications. Regardless, blocking the flow of traffic into and out of U.S. information infrastructure would require the assistance of many private Internet service providers (ISPs), as there is no single, government-owned national network. The bill's sponsors wrote that such authorities already exist for the President to compel private companies to suspend service, particularly in the Communications Act of 1934, and the new legislation would actually limit presidential emergency powers over the Internet. A new proposal in the 112th Congress, S. 413,

[45] The White House, *National Security Strategy*, May 2010, accessed at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[46] See, for example, U.S. Senate, Committee on Homeland Security and Governmental Affairs, hearing, *The Internet: A Portal to Violent Islamist Extremism*, May 3, 2007, and U.S. House, Subcommittee on Intelligence, *Information Sharing and Terrorism Risk Assessment, hearing on Using the Web as a Weapon: the Internet as a Tool for Violent Radicalization and Homegrown Terrorism*, November 6, 2007.

[47] A copy of the letter can be accessed at http://mountainrunner.us/files/2010-3-2_SCPD_Caucus_Announcmement.pdf.

the Cybersecurity and Internet Freedom Act of 2011, contains a provision that would amend the Communications Act of 1934 so that, "[n]otwithstanding any provision of this Act, an amendment made by this Act, or section 706 of the Communications Act of 1934 (47 U.S.C. 606), neither the President, the Director of the National Center for Cybersecurity and Communications, or any officer or employee of the United States Government shall have the authority to shut down the Internet."

The Communications Decency Attack of 1996 (CDA), codified in Title V of the Telecommunications Act of 1996, was an effort to regulate both indecency and obscenity in cyberspace. Although much of it is targeted at lewd or pornographic material, particularly when shown to children under the age of 18, the law's definition of obscenity and harassment could also be interpreted as applying to graphic, violent terrorist propaganda materials or incendiary language.[48] YouTube's terms of use (called "Community Guidelines") prohibit, among other things, "gratuitous and graphic violence" and "hate speech."[49] To control its content, YouTube employs a user-feedback system, where users flag potentially offensive videos that are then reviewed and removed by the site's administrators. However, Section 230 of the CDA reads: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This would absolve both ISPs and Internet administrators from liability for the words or crimes committed by third-party users of their websites or online forums, even if the provider or administrator fails to take action after receiving notice of the harmful or offensive content. In other words, although many ISPs and website administrators follow internal policies that restrict the type of material posted on their sites or trafficked through their networks, they may not have a legal responsibility to dismantle a site with offensive or violent content.

In September 2010, General Alexander told the House Armed Services Committee that the White House was leading an effort to review the legal framework governing operations in cyberspace and the protection of telecommunications infrastructure.[50] The results of this review will be presented to Congress, with legislative recommendations on what new statutes may be required and which should be revised or amended to facilitate effective operations in cyberspace. The 2011 National Military Strategy also contains a point to that effect.[51]

[48] In a 2008 letter to Google CEO Eric Schmidt, Senator Joseph Lieberman, Chairman of the Homeland Security and Governmental Affairs Committee, appealed to Google's sense of decency in urging the company to take down violent extremists' YouTube videos that Google hosted. See http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=8093d5b2-c882-4d12-883d-5c670d43d269&Region_id=&Issue_id=716b4c83-7747-4193-897b-632e5c281a91.

[49] See YouTube's Community Guidelines here: http://www.youtube.com/t/community_guidelines.

[50] Hearing before the House Armed Services Committee on *U.S. Cyber Command: Organizing for Cyberspace Operations*, September 23, 2010.

[51] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America*, February 8, 2011, accessed at http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.

Author Contact Information

Catherine A. Theohary
Analyst in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844

John Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529