6

Terrorism and the Internet

Should Web Sites That Promote Terrorism Be Shut Down?

Barbara Mantel

AP Photo/Ellis County Sheriff's Department

Hosam Maher Husein Smadi, a Jordanian teenager in the United States illegally, pleaded not guilty on Oct. 26 of trying to blow up a 60-story Dallas skyscraper. Smadi reportedly parked a vehicle in the building's garage on Sept. 24 hoping to detonate explosives with a cellphone. FBI agents, posing as al-Qaeda operatives, had been keeping tabs on Smadi after discovering him on an extremist Web site earlier this year where he stood out for "his vehement intention to actually conduct terror attacks in the United States."

From *CQ Researcher*,
November 2009.

In March 2008 a participant on the pro al-Qaeda online forum ek-Is.org posted six training sessions for aspiring terrorists. The first was entitled: "Do you want to form a terror cell?" Using the name Shamil al-Baghdadi, the instructor described how to choose a leader, recruit members and select initial assassination targets. The second lesson outlined assassination techniques.[1]

"Although the first two training lessons often contain very basic instructions that may be less significant for experienced jihadis, they provide essential training for novices," said Abdul Hameed Bakier, a Jordanian terrorism expert who translated and summarized the training manual.[2]

The sessions then progressed to more sophisticated topics. Lesson three explained in more detail how to carry out assassinations, including: suicide attacks using booby-trapped vehicles or explosive belts; sniper attacks using Russian, Austrian and American rifles and direct attacks through strangling, poison and booby-trapped cellular phones.[3] Lesson four explained how to steal funds, and the final two lessons gave detailed instructions on how to conduct "quality terror attacks," including strikes against U.S. embassies.[4]

While this particular forum can no longer be accessed under its original domain name, Web sites controlled or operated by terrorist groups have multiplied dramatically over the past decade.

"We started 11 years ago and were monitoring 12 terrorist Web sites," says Gabriel Weimann, a professor of communication at Haifa University in Israel and a terrorism researcher. "Today we are monitoring more than 7,000."

Analysts say nearly every group designated as a foreign terrorist organization by the U.S. State Department now has an online presence, including Spain's Basque ETA movement, Peru's Shining Path, al Qaeda, the Real Irish Republican Army and others.[5] (*See list, p. 131.*)

The Internet appeals to terrorists for the same reasons it attracts everyone else: It's inexpensive, easily accessible, has little or no regulation, is interactive, allows for multimedia content and the potential audience is huge.[6] And it's anonymous.

"You can walk into an Internet café, enter a chat room or Web site, download instructions to make a bomb, and no one can find you," says Weimann. "They can trace you all the way down to the computer terminal, but by then you'll already be gone."

Terrorism on the Internet extends far beyond Web sites directly operated or controlled by terrorist organizations. Their supporters and sympathizers are increasingly taking advantage of all the tools available on the Web. "The proliferation of blogs has been exponential," says Sulastri Bte Osman, an analyst with the Civil and Internal Conflict Programme at Nanyang Technological University in Singapore. Just two years ago, Osman could find no extremist blogs in the two predominant languages of Indonesia and Malaysia; today she is monitoring 150.

The University of Arizona's "Dark Web" project, which tracks terrorist and extremist content in cyberspace, estimates there are roughly 50,000 such Web sites, discussion forums, chat rooms, blogs, Yahoo user groups, video-sharing sites, social networking sites and virtual worlds.[7] They help to distribute content — such as videos of beheadings and suicide attacks, speeches by terrorist leaders and training manuals — that may originate on just a few hundred sites.

Security experts say terrorist groups use the Internet for five general purposes:

- **Research and communication:** The Sept. 11, 2001, terrorists who attacked the World Trade Center and the Pentagon used the Internet to research flight schools, coordinate their actions through e-mail and gather flight information.[8]
- **Training:** Global Islamic Media Front, a propaganda arm of al Qaeda, issued a series of 19 training lessons in 2003 covering topics like security, physical training, weapons and explosives. The document was later found on a computer belonging to the terrorist cell responsible for the 2004 train bombings in Madrid, Spain, that killed 191 people. But most material is posted by individuals who use the Internet as a training library.[9]
- **Fundraising:** In 1997 the rebel Tamil Tigers in Sri Lanka stole user IDs and passwords from faculty at Britain's Sheffield University and used the e-mail accounts to send out messages asking for donations.[10]
- **Media operations:** Before his death in 2006, Abu Musab al Zarqawi, the mastermind behind hundreds of bombings, kidnappings and killings in Iraq, posted gruesome videos of terrorist operations, tributes immortalizing suicide bombers and an Internet magazine offering religious justifications for his actions.[11]
- **Radicalization and recruitment:** In 2006, Illinois resident Derrick Shareef pleaded guilty to attempting to acquire explosives to blow up a mall in Rockford, Ill. Although not part of a terrorist organization, he was inspired in part by violent videos downloaded from a Web site linked to al Qaeda.[12]

The use of the Internet for recruitment and radicalization particularly worries some authorities. But experts disagree over the extent to which cyber content can radicalize and convert young men and women into homegrown supporters of — or participants in — terrorism.

The Internet is where "the gas meets the flame," says Evan F. Kohlmann, a senior investigator with the NEFA Foundation, a New York-based terrorism research organization.* "It provides the medium where would-be megalomaniacs can try and recruit deluded and angry young men . . . and magnify that anger to convince them to carry out acts of violence." The Internet replaces and broadens the traditional social networks of mosques and Arabic community centers, which have come under intense government scrutiny since 9/11, says Kohlmann.

A frequent expert witness in terrorism cases, Kohlmann says the Internet comes up in nearly every prosecution. For instance, Hamaad Munshi — a British national convicted in 2008 of possessing materials likely to be used for terrorism — participated in an online British extremist group that shared terrorist videos and used chat rooms to discuss its plans to fight overseas.[13] He was arrested at age 16.

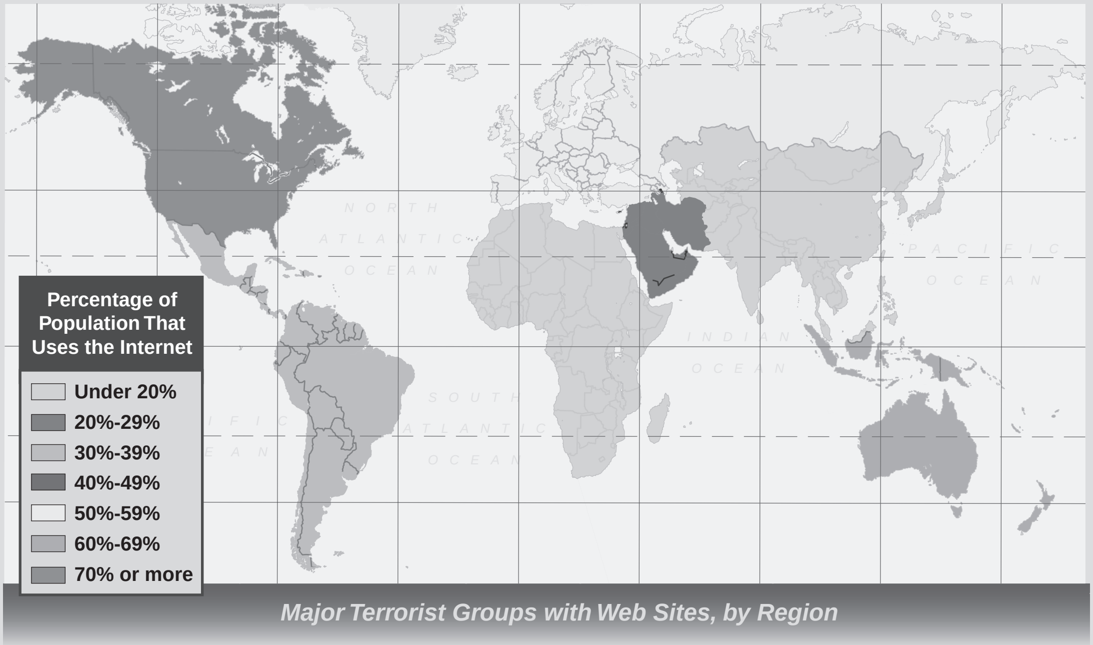
The group's ringleader, then 22-year-old Aabid Khan, another Briton, used the chat rooms to incite Munshi to fight, Kohlmann says; the youth's grandfather also

* NEFA stands for "Nine Eleven Finding Answers."

Internet Offers Vast Potential for Spreading Terror

The Internet has opened global communication channels to anyone with computer access, creating a simple and cheap venue for spreading terrorist ideology. Interestingly, the regions with the largest concentrations of terrorist groups — the Middle East and Asia — have some of the lowest Internet usage rates. The highest rates are in developed countries, such as the United States, Canada, Australia and New Zealand.

World Internet Usage Rates, by Region



Major Terrorist Groups with Web Sites, by Region

Middle East: *Hamas, Lebanese Hezbollah, al-Aqsa Martyrs Brigades, Fatah Tanzim, Popular Front for the Liberation of Palestine, Palestinian Islamic Jihad, Kahane Lives Movement, People's Mujahidin of Iran, Kurdish Workers' Party, Popular Democratic Liberation Front Party, Great East Islamic Raiders Front*

Europe: *Basque Euskadi Ta Askatasuna, Armata Corsa, Real Irish Republican Army*

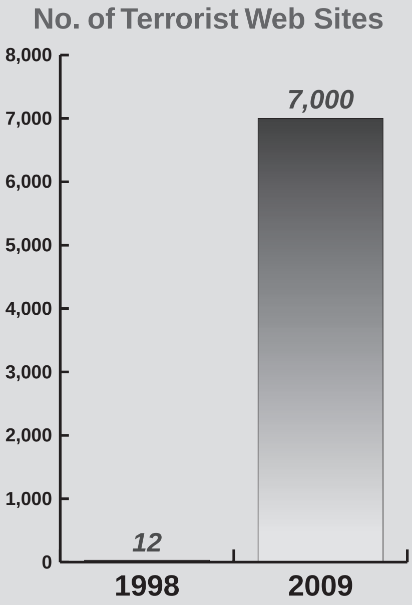
Latin America: *Tupac-Amaru, Shining Path, Colombian National Liberation Army, Armed Revolutionary Forces of Colombia, Zapatista National Liberation Army*

Asia: *Al Qaeda, Japanese Supreme Truth, Ansar al Islam, Japanese Red Army, Hizb-ul Mujahidin, Liberation Tigers of Tamil Eelam, Islamic Movement of Uzbekistan, Moro Islamic Liberation Front, Lashkar-e-Taiba, Chechnyan Rebel Movement*

Sources: "World Internet Penetration Rates by Geographic Region," Internet World Stats, June 30, 2009, www.internetworldststs.com/stats.htm; Gabriel Weimann, "Terror on the Internet," 2006

Terrorist Web Sites Have Proliferated

The number of Web sites run by terrorists or their supporters has grown since 1998 from a dozen to more than 7,000, with pro-jihad sites predominating, according to researcher Gabriel Weimann of Israel's Haifa University.



Source: Gabriel Weimann, Haifa University, Oct. 20, 2009

blamed the Internet. "This case demonstrates how a young, impressionable teenager can be groomed so easily through the Internet to associate with those whose views run contrary to true Muslim beliefs and values," Yakub Munshi said after the teen's conviction.[14]

But other researchers say online terrorism sites are largely about preaching to the choir and have limited influence on non-terrorists. "There has been very little evidence that the Internet has been the main or sole driver in radicalization," says Peter Neumann, director of the International Centre for the Study of Radicalisation and Political Violence at King's College in London. "In most cases, radicalization requires would-be terrorists to come in contact with social groups of people in the real world."

For instance, he pointed out, while much of Munshi's extremist activism took place online, "his radicalisation had been initiated in the 'real world.' " Through a friend at a local mosque, Munshi had met Khan, who spotted Munshi's computer expertise and groomed him to become a part of his online network. "It was the early meetings with Khan and some of his friends that helped turn a boy interested in religion into a young man dedicated to killing 'non-believers,' " according to Neumann.[15]

"There is anecdotal evidence out there, but no one has done a systematic study to show that radicalization via the Internet is a reality," says Maura Conway, a terrorism expert at Dublin City University in Ireland. Nevertheless, she adds, "governments are certainly acting as if radicalization through the Internet is possible, putting in place legislation that curbs how people can interact online."

As terrorists' presence on the Internet continues to grow, here are some of the questions being asked:

Should governments block terrorist Web sites?

Many of those who think the Internet is a major terrorist recruiting tool say authorities should simply shut down terrorists' sites.

Often the call comes from politicians. "It is shocking the government has failed to shut down a single Web site, even though Parliament gave them that power," Britain's opposition security minister, Baroness Pauline Neville-Jones, said last March. "This smacks of dangerous complacency and incompetence."[16]

In France, a minister for security said she wanted to stop terrorist propaganda on the Internet.[17] And a European Commission official called for a Europe-wide prohibition on Web sites that post bomb-making instructions.[18]

Although governments have shut down terrorist Web sites when they felt the information posted was too great a threat, some critics say such a move is legally complicated, logistically difficult and unwise.

Last year, three of the most important discussion forums used by Islamist terrorist groups disappeared from the Internet, including ek-Is.org, which had posted the six-part training manual. Jordanian terrorism expert

Bakier says counterterrorism officials were so worried about the site that he "used to get requests from concerned agencies to translate the exact texts posted on ek-Is.org that were referenced in my articles. It was that serious."

"It is widely assumed that Western intelligence agencies were responsible for removing the three sites," and probably without the cooperation of the Internet service providers (ISPs) that host the sites, says Neumann, of King's College. "It would have required the cooperation of all the ISPs in the world," because those Web sites were not accessible at all, he explains. Instead, he thinks intelligence agencies may have launched so-called denial-of-service attacks against the sites, bombarding them with so many requests that they crashed. This September, one of the sites resurfaced; however, many experts believe it is a hoax.[19]

But government takedowns of terrorist sites — by whatever method — are not common, say many researchers. First, there are concerns about free speech.

"Who is going to decide who is a terrorist, who should be silenced and why?" asks Haifa University's Weimann. "Who is going to decide what kind of Web site should be removed? It can lead to political censorship."

Concern about free speech may be more acute in the United States than elsewhere. Current U.S. statutes make it a crime to provide "material support" — including expert advice or assistance — to organizations designated as terrorist groups by the State Department.[20] However, the First Amendment guarantee of free speech may trump the material support provisions.

"Exceptions to the First Amendment are fairly narrow" says Ian Ballon, an expert on Internet law practicing in California. "Child pornography is one, libelous or defamatory content another. There is no terrorism exception per se." Words that would incite violence are clearly an exception to the First Amendment, he says, "but there is a concept of immediacy, and most terrorism sites would not necessarily meet that requirement." A 1969 Supreme Court case, *Brandenburg v. Ohio*, held that the government cannot punish inflammatory speech unless it is inciting or likely to incite imminent lawless action.[21]

In Europe, where free-speech rights are more circumscribed than in the United States, the legal landscape varies. Spain, for instance, outlaws as incitement "the act of performing public ennoblement, praise and/or justification of a terrorist group, operative or act," explains Raphael Perl, head of the Action Against Terrorism Unit at the Organization for Security and Co-operation in Europe, a regional security organization with 56 member nations, based in Vienna, Austria. And the U.K. passed the Terrorism Acts of 2000 and 2006, which make it an

AP Photo/Keystone/Karl Mathis

Tunisian Moez Garsallaoui, right, and his wife Malika El Aroud, the widow of an al-Qaeda suicide bomber, were convicted in Switzerland's first Internet terrorism trial of running pro-al-Qaeda Web sites that showed executions. Garsallaoui served three weeks in prison; El Aroud received no jail time. They are continuing their online work from Belgium, where El Aroud is described by Belgian State Security chief Alain Winants as a "leading" Internet jihadist.

AP Photo/Matt Dunham-WPA Pool

British officials, including Prime Minister Gordon Brown, center right, visit a London cyber security firm on June 25 during the launch of a new government campaign to counter cyber criminals and terrorists.

Southeast Asian Sites Now Espouse Violence

Extremist Web sites using the two main languages in Indonesia and Malaysia have evolved since 2006 from mostly propagandizing to providing firearm and bomb-making manuals and encouraging armed violence.

How the Sites Evolved

2006-July 2007	Posted al-Qaeda and Jemaah Islamiyah propaganda (videos, photographs, statements, etc.); articles about how Muslims are victimized and the necessity to fight back; celebrations of mujahidin victories; conspiracy theories; anger directed at the West; local grievances linked to global jihad; endorsements of highly selective Islamic doctrines
August 2007	First posting of manual on how to hack Web sites
February 2008	First posting of bomb-making manual and bomb-making video compilation in Arabic; emergence of a password-protected forum
April 2008	First posting of a firearm manual
Present	All of the above posted/available

Source: "Contents of Bahasa and Malay Language Radical and Extremist Web Sites, 2006 to 2009," in "Countering Internet Radicalisation in Southeast Asia," S. Rajaratnam School of International Studies, Singapore, and Australian Strategic Policy Institute, 2009

offense to collect, make or possess material that could be used in a terrorist act, such as bomb-making manuals and information about potential targets. The 2006 act also outlaws the encouragement or glorification of terrorism.[22] Human Rights Watch says the measure is unnecessary, overly broad and potentially chilling of free speech.[23]

Yet, it does not appear that governments are using their legal powers to shut down Web sites. "I haven't heard from any ISP in Europe so far that they have been asked by the police to take down terrorist pages," says Michael Rotert, vice president of the European Internet Service Providers Association (EuroISPA).

For one thing, says Rotert, there is no common, legal, Europe-wide definition of terrorism. "We are requesting a common definition," he says, "and then I think notice and takedown procedures could be discussed. But right now, such procedures only exist for child pornography."

But even if a European consensus existed on what constitutes terrorism, the Internet has no borders. If an ISP shuts down a site, it can migrate to another hosting service and even register under a new domain name.

Instead of shutting down sites, some governments are considering filtering them. Germany recently passed a filtering law aimed at blocking child pornography, which it says could be expanded to block sites that promote terrorist acts. And Australia is testing a filtering system for both child pornography and material that advocates terrorism.

The outcry in both countries, however, has been tremendous, both on technical grounds — filtering can slow down Internet speed — and civil liberties grounds. "Other countries using similar systems to monitor Internet traffic have blacklisted political critics," wrote an Australian newspaper columnist. "Is this really the direction we want our country to be heading? Communist China anyone? Burma? How about North Korea?"[24]

Ultimately, filtering just may not be that effective. Determined Internet users can easily circumvent a national filter and access banned material that is legal elsewhere. And filtering cannot capture the dynamic parts of the Internet: the chat rooms, video sharing sites and blogs, for instance.

Even some governments with established filtering laws seem reluctant to remove terrorist sites. The government owns Singapore's Internet providers and screens all Web sites for content viewed as " 'objectionable' or a potential threat to national security."[25] Yet Osman, of the Nanyang Technological University, says the government is not blocking Web sites that support terrorism. "I can still get access to many of them," she says, "so a lot of other people can, too."

In fact, counterterrorism officials around the world often prefer to monitor and infiltrate blogs, chat rooms, discussion forums and other Web sites where terrorists and sympathizers converse. If the sites remain active, they can be mined for intelligence.

"One reason [for not shutting down sites] is to take the temperature, to see whether the level of conversation is going up or down in terms of triggering an alert among security agencies," says Anthony Bergin, director of research at the Australian Strategic Policy Institute.

Another purpose is to disrupt terrorist attacks, says Bergin. Just recently, the violent postings of Texas resident Hosan Maher Husein Smadi to an extremist chat room attracted the attention of the FBI, which was monitoring the site. Agents set up a sting operation and arrested the 19-year-old Jordanian in late September after he allegedly tried to detonate what he thought was a bomb, provided by an undercover agent, in the parking garage beneath a Dallas skyscraper.[26]

Should Internet companies do more to stop terrorists' use of the Web?

Between 100 and 200 Web sites are the core "fountains of venom," says Yigal Carmon, president of the Middle East Media Research Institute, headquartered in Washington, D.C., with branch offices in Europe, Asia and the Middle East. "All the rest, are replication and duplication. You need to fight a few hundred sites, not thousands."

And many of these sites, he says, are hosted in the West. American hosting services, for instance, are often cheaper, have sufficient bandwidth to accommodate large video files and enjoy free-speech protection. But the companies often don't know they are hosting a site that, if not illegal, is perhaps violating their terms-of-service agreements.

Most Internet Service Providers, Web hosting companies, file-sharing sites and social networking sites have terms-of-service agreements that prohibit certain content. For instance, the Yahoo! Small Business Web hosting service states that users will not knowingly upload, post, e-mail, transmit or otherwise distribute any content that is "unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful or racially, ethnically or otherwise objectionable."

It also specifically forbids users from utilizing the service to "provide material support or resources . . . to any organization(s) designated by the United States government as a foreign terrorist organization."

But Yahoo! also makes clear that it does not pre-screen content and that "You, and not Yahoo!, are entirely responsible for all Content that you upload, post, transmit, or otherwise make available."[27]

Some policy makers want Internet companies to begin screening the sites they host. Last year in the U.K., for instance, the House of Commons's Culture, Media and Sport Select Committee recommended that the "proactive review of content should be standard practice for sites hosting user-generated content."[28]

Internet companies, as well as civil libertarians and privacy advocates, disagree. "We do not think that ISPs should monitor anything since they are just in the business of transferring bits and bytes," says Rotert of EuroISPA. "We still believe in privacy laws."

David McClure, president and CEO of the U.S. Internet Industry Association, concurs. "If I'm a Web hoster, it is not my job to go snooping through the files and pages that people put on those Web sites," says McClure. "It's my job to keep the servers and the hosting service running." And, according to McClure, no U.S. law compels them to do more. Under the Telecommunications Act of 1996, McClure says, companies that host Web sites are not legally responsible for their content.

Still, ISPs and Web hosting companies do remove sites that violate their terms-of-service agreements, once they are aware of them. Since 9/11 a variety of private watchdog groups — like the SITE Intelligence Group and Internet Haganah — have made it their business to track jihadi Web sites.

Some anti-jihadist activists, like Aaron Weisburd — who created and runs Internet Haganah — have even contacted ISPs in an effort to shame them into taking down sites. Perhaps hundreds of sites have been removed with his help. "It is rare to find an Internet company that does not care or that actively supports the terrorist cause," he says.

Weisburd says some sites should be left online because they are good sources of intelligence, "while many other sites can — and arguably should — be taken down." He says the main reason to remove them is not to get them off the Internet permanently — which is extremely difficult to do — but to track individuals as they open new accounts in order to gather evidence and prosecute them.

AP Photo/Sankei Shimbum/Kiyohiro Oku

Members of the Peruvian revolutionary movement Tupac Amaru flash victory signs after seizing the Japanese ambassador's residence in Lima in December 1996, along with hundreds of hostages. The morning after the seizure, the rebels launched a new era in terrorist media operations by posting a 100-page Web site, based in Germany. As the four-month siege dragged on, the group updated the site periodically, using a laptop and a satellite telephone. The hostages were eventually rescued in a raid by the Peruvian military.

But ISPs don't always follow through. "Even when you get a complaint about a Web site that may be violating the terms of service, many Web hosting services may be unlikely to pursue it," says McClure. Investigating complaints is time-consuming and expensive, he says, and "once you start pursuing each complaint, you are actively involved in monitoring, and the complaints will skyrocket."

To monitor how the big Internet platforms respond to user complaints, Neumann, of King's College, suggests forming an Internet Users Panel, which could name and shame companies that don't take users' complaints seriously. "We don't want the panel to be a government body," says Neumann. "We are proposing a body that consists of Internet users, Internet companies and experts." It could publicize best practices, he says, and act as an ombudsman of last resort. ISPs would fund the panel.

But Neumann's proposal does not sit well with the ISPs. "A lot of people propose that ISPs do a lot of things," says McClure, "and what they want is for ISPs to do a lot of work for nothing."

Carmon also objects to relying on ISPs and Web hosting companies to respond to user complaints. "It's a totally untrustworthy system because you don't know who is making the complaint and why," Carmon says. "I issue a complaint against your Web site, but I may be settling an account against you, I may be your competitor in business." So ISPs must be very careful in evaluating complaints, which takes time, he says; ISPs don't want to be sued.

Instead, Carmon proposes creating what he calls a Civic Action Committee, based at an accredited research organization, which would monitor the Web and recommend sites that ISPs should consider closing. The committee would be made up of "intellectuals, writers, authors, people known for their moral standing, activists and legislators from different political parties," says Carmon.

Rotert is doubtful. "The ISPs in Europe would follow only government requests for notice and takedown procedures," he says, "because the ISPs know they cannot be held liable for destroying a business by taking down a site if the order came from the police."

Conway, of Dublin City University, has another objection to private policing of the Internet. "The capacity of private, political and economic actors to bypass the democratic process and to have materials they find politically objectionable erased from the Internet is a matter of concern," she said. Governments might want to consider legislation not just to regulate the Internet — "perhaps, for example, outlawing the posting and dissemination of beheading videos — but also writing into law more robust protections for radical political speech."[29]

Does cyberterrorism pose a serious threat?

Last year Pakistani President Asif Ali Zardari issued the following decree: "Whoever commits the offence of cyberterrorism and causes death of any person shall be punishable with death or imprisonment for life."[30]

In March India's cabinet secretary warned an international conference that cyber attacks and cyberterrorism are looming threats. "There could be attacks on critical infrastructure such as telecommunications, power distribution, transportation, financial services, essential public utility services and others," said K. M. Chandrasekhar. "The damage can range from a simple shutdown of a computer system to a complete paralysis of a significant portion of critical infrastructure in a specific region or even the control nerve centre of the entire infrastructure."[31]

Politicians, counterterrorism officials and security experts have made similarly gloomy predictions about cyberterrorism since 9/11 — and even before. But to date there have been no such attacks, although an ex-employee of a wastewater treatment plant in Australia used a computer and a radio transmitter to release sewage into parks and resort grounds in 2000.

Cyberterrorism is generally defined as highly damaging computer attacks by private individuals designed to generate terror and fear to achieve political or social goals. Thus, criminal hacking — no matter how damaging — conducted to extort money or for bragging rights is not considered cyberterrorism. (Criminal hacking is common. A year ago, for instance, criminals stole personal credit-card information from the computers of RBS WorldPay and then used the data to steal $9 million from 130 ATMs in 49 cities around the world.[32]) Likewise, the relatively minor denial-of-service attacks and Web defacements typically conducted by hackers aligned with terrorist groups also are not considered cyberterrorism.[33]

Skeptics say cyberterrorism poses only a slim threat, in part because it would lack the drama of a suicide attack or an airplane crash. "Let's say terrorists cause the lights to go out in New York City or Los Angeles, something that has already happened from weather conditions or human error," says Conway, of Dublin City University. "That is not going to create terror," she says, because those systems have been shown they can rapidly recover. Besides, she adds, terrorist groups tend to stick with what they know, which are physical attacks. "There is evolution but not sea changes in their tactics."

Even if terrorists wanted to launch a truly destructive and frightening cyber attack, their capabilities are very limited, says Irving Lachow, a senior research professor at the National Defense University in Washington, D.C. "They would need a multidisciplinary team of people to pull off a cyberterrorism attack," he says.

"A lot of these critical facilities are very complicated, and they have hundreds of systems," he continues. To blow up a power plant, for instance, a terrorist group would need an insider who knows which key computer systems are vulnerable, a team of experienced hackers to break into these systems, engineers who understand how the plant works so real damage can be done, a computer simulation lab to practice and lots of time, money and secrecy.

"At the end of the day, it's a lot easier just to blow something up," Lachow says.

But others fear that as governments continue to foil physical attacks, terrorists will expand their tactics to include cyberterrorism. Some analysts warn that terrorists could purchase the necessary expertise from cyber criminals. That, said Steven Bucci, IBM's lead researcher for cyber security, would be "a marriage made in Hell."[34]

According to Bucci, cybercrime is "a huge (and still expanding) industry that steals, cheats and extorts the equivalent of many billions of dollars every year." The most insidious threat, he said, comes from criminal syndicates that control huge botnets: worldwide networks of unwitting personal computers used for denial-of-service attacks, e-mail scams and distributing malicious software.[35]

The syndicates often rent their botnets to other criminals. Some analysts fear it's only a matter of time before a cash-rich terrorist group hires a botnet for its own use. "The cyber capabilities that the criminals could provide would in short order make any terrorist organization infinitely more dangerous and effective," said Bucci, and the permutations are "as endless as one's imagination." For example, terrorists could "open the valves at a chemical plant near a population center," replicating the deadly 1984 chemical accident in Bhopal, India.[36]

And a full-fledged cyberterrorism attack is not the only disturbing possibility, say Bucci and others. Perl at the Organization for Security and Co-operation believes terrorists are much more likely to use a cyber attack to amplify the destructive power of a physical attack. "One of the goals of terrorism is to create fear and panic," says Perl, "and not having full access to the Internet could greatly hamper governments' response to a series of massive, coordinated terrorist incidents." For example, terrorists might try to disable the emergency 911 system while blowing up embassies.

Some experts are particularly concerned that al Qaeda could launch a coordinated attack on key ports while simultaneously disabling their emergency-response systems, in order to immobilize the trade-dependant global economy. Al-Qaeda leaders have made it clear that destroying the industrialized world's economy is one of the group's goals.

But Dorothy Denning, a professor of conflict and cyberspace at the Naval Postgraduate School in Monterey, Calif., said, "Terrorists do not normally integrate

Governments Now Prosecute Suspected Online Terrorists

New laws apply to online activities.

Governments around the world have prosecuted suspected terrorists before they carry out acts of violence, but not many have been prosecuted solely for their alleged online activities in support of terrorism.

Those cases have been hampered by concerns about restricting free speech, the desire to monitor terrorist-linked sites for intelligence and the difficulty of identifying individuals online. Here are some examples of such cases:

Sami Al-Hussayen — A 34-year-old graduate student in computer science at the University of Idaho, Al-Hussayen was arrested in February 2003 and accused of designing, creating and maintaining Web sites that provided material support for terrorism. It was the U.S. government's first attempt at using statutes prohibiting material support for terrorism to prosecute activity that occurred exclusively online. The definition of "material support" used by the prosecutors had been expanded under the Patriot Act of 2001 to include "expert advice or assistance."

Al-Hussayen had volunteered to run Web sites for two Muslim charities and two Muslim clerics. But prosecutors alleged that messages and religious fatwas on the sites encouraged jihad, recruited terrorists and raised money for foreign terrorist groups. It didn't matter that Al-Hussayen had never committed a terrorist act or that he hadn't written the material. Prosecutors said it was enough to prove that he ran the Web sites and knew the messages existed.

Jurors were not convinced, however. They acquitted Al-Hussayen in June 2004. "There was no direct connection in the evidence they gave us — and we had boxes and boxes to go through — between Sami and terrorism," said one juror.[1]

The case attracted national attention, and according to University of Idaho law professor Alan Williams, "triggered a heated debate focused mainly on a key question: Were Al-Hussayen's Internet activities constitutionally protected free speech or did they cross the line into criminal and material support to terrorism?"[2]

The U.S. Supreme Court is scheduled to hear challenges to the material support statute — which critics complain is too vague — in two related cases this session.[3]

Younis Tsouli — In late 2005, British police arrested 22-year-old Tsouli, a Moroccan immigrant and student who prosecutors alleged was known online as "Irhaby 007" — or Terrorist 007. The government linked Tsouli and his accomplices Waseem Mughal and Tariq al-Daour to "the purchase, construction and maintenance of a large number of Web sites and Internet chat forums on which material was published which incited acts of terrorist murder, primarily in Iraq."[4]

Tsouli had been in active contact with al Qaeda in Iraq and was part of an online network that extended to Canada, the United States and Eastern Europe. In July 2007, Tsouli, Mughal and Al-Daour "became the first men to plead guilty to inciting murder for terrorist purposes" under the U.K.'s Terrorism Act of 2000.[5]

Samina Malik — In November 2007 the 23-year-old shop assistant became the first woman convicted of terrorism in the United Kingdom when she was found guilty of "possessing information of a kind likely to be useful to a person committing or preparing an act of terrorism."[6]

Malik had downloaded and saved on her hard drive *The Terrorist's Handbook*, *The Mujahideen Poisons Handbook* and other documents that appeared to support violent jihad.

multiple modes of attack." If coordinating cyber and physical attacks did become their goal, Denning would expect to see evidence of failed attempts, training, discussions and planning. "Given terrorists' capabilities today in the cyber domain, this seems no more imminent than other acts of cyberterror," she said. "At least in the near future, bombs remain a much larger threat than bytes."[37]

But that doesn't mean critical infrastructure is secure from cyber criminal syndicates or nation-states, which do have the technical know-how, funds and personnel to launch a damaging attack, Denning said. "Even if our critical infrastructures are not under imminent threat by terrorists seeking political and social objectives," she said, "they must be protected from harmful attacks conducted for other reasons, such as money, revenge, youthful curiosity and war."[38]

She had also written violent poems about killing nonbelievers. Her defense portrayed her as a confused young woman assuming a persona she thought was "cool."

Her conviction sparked public outrage. Muhammed Abdul Bari, secretary general of the Muslim Council of Britain, said, "Many young people download objectionable material from the Internet, but it seems if you are Muslim then this could lead to criminal charges, even if you have absolutely no intention to do harm to anyone else." An appeals court later overturned her conviction and clarified a new requirement that suspects must have a clear intent to engage in terrorism.[7]

Ibrahim Rashid — In 2007 German prosecutors charged the Iraqi Kurdish immigrant with waging a "virtual jihad" on the Internet. They argued that by posting al-Qaeda propaganda on chat rooms, Rashid was trying to recruit individuals to join al Qaeda and participate in jihad. It was Germany's first prosecution of an Islamic militant for circulating propaganda online.[8]

"This case underscores how thin the line is that Germany is walking in its efforts to aggressively target Islamic radicals," wrote Shawn Marie Boyne, a professor at Indiana University's law school. "While active membership in a terrorist organization is a crime . . . it is no longer a crime to merely sympathize with terrorist groups or to distribute propaganda."[9] Thus, the prosecution had to prove that Rashid's postings went beyond expressing sympathy and extended to recruiting. The court found him guilty in June 2008.

Saïd Namouh — On Oct. 1, the 36-year-old Moroccan resident of Quebec was convicted under Canada's Anti-Terrorism Act of four charges largely related to his online activities. In March 2007 he had helped publicize a video warning Germany and Austria that they would suffer a bomb attack if they didn't withdraw their troops from Afghanistan. He also distributed violent videos on behalf of Global Islamic Media Front, a propaganda arm of al Qaeda. Intercepted Internet chats revealed Namouh's plans to explode a truck bomb and die a martyr. "Terrorism is in our blood, and with it we will drown the unjust," Namouh said online.[10]

AFP/Getty Images

Tariq al-Daour, Younis Tsouli and Waseem Mughal (left to right), in 2007 became the first to plead guilty to inciting murder for terrorist purposes online under the U.K.'s Terrorism Act of 2000.

— Barbara Mantel

[1] Maureen O'Hagan, "A terrorism case that went awry," seattletimes.com, Nov. 22, 2004, http://seattletimes.nwsource.com/html/localnews/2002097570_sami22m.html.

[2] Alan Williams, "Prosecuting Website Development Under the Material Support in Terrorism Statutes: Time to Fix What's Broken," *NYU Journal of Legislation & Public Policy*, 2008, p. 366.

[3] The cases are *Holder v. Humanitarian Law Project*; *Humanitarian Law Project v. Holder*, 08-1498; 09-89. See http://onthedocket.org/cases/2009.

[4] Elizabeth Renieris, "Combating Incitement to Terrorism on the Internet: Comparative Approaches in the United States and United Kingdom and the Need for an International Solution," *Vanderbilt Journal of Entertainment and Technology Law*, vol. 11:3:673, p. 698, 2009.

[5] *Ibid.*

[6] *Ibid.*

[7] *Ibid.*, pp. 699-700.

[8] Shawn Marie Boyne, "The Criminalization of Speech in an Age of Terror," working paper, June 12, 2009, p. 7, http://ssrn.com/abstract=1418496.

[9] *Ibid.*

[10] Graeme Hamilton, "Quebec terror plotter undone by online activities," *National Post*, Oct. 1, 2009, www.nationalpost.com/news/story.html?id=2054720.

BACKGROUND

Growth and Evolution

After seizing the Japanese embassy in Lima, Peru, on Dec. 17, 1996, the Tupac Amaru communist rebels "launched a new era in terrorist media operations," wrote Denning. The next morning the group had a Web site with more than 100 pages up and running out of Germany, which it updated using a laptop and a satellite telephone.[39]

"For the first time, terrorists could bring their message to a world audience without mediation by the established press or interference by the government," Denning said. They could offer the first news accounts to the media, and they could use the Web site to communicate directly with their members and supporters. "The advantage the

CHRONOLOGY

1990s *Terrorist groups discover the Internet's usefulness for fundraising and publicity.*

1996 After seizing the Japanese embassy in Lima, Peruvian revolutionary movement Tupac Amaru creates a Web site to publicize its actions.

1997 Sri Lanka's Tamil Tigers use stolen Sheffield University faculty members' computer IDs and passwords to solicit donations.

1998 Researchers looking for online terrorism sites discover al Qaeda's Web site, www.alneda.com.

1999 Nearly all 30 U.S.-designated foreign terrorist organizations have an Internet presence.

2000-2005 *Extremist Web sites and discussion forums multiply; first prosecution of man accused of providing material online in support of terrorists fails.*

July 20, 2000 Terrorism Act of 2000 makes it illegal in the U.K. to collect, make or possess information likely to be used in terrorism.

2001 The 9/11 attackers use the Internet to research flight schools and flights and to coordinate their actions. On Oct. 26, 2001, President George W. Bush signs the USA Patriot Act, which prohibits "material support" for terrorists.

2003 Abdelaziz al-Muqrin, leader of al Qaeda in Saudi Arabia, pioneers several digital magazines, including *Sawt al-Jihad* (*The Voice of Jihad*).

2004 Video of the decapitation of kidnapped U.S. businessman Nicholas Berg is released on a Malaysian Web site. . . . University of Idaho graduate student Sami Omar al-Hussayen is acquitted of fostering terrorism online after his lawyers raise freedom of expression issues. Autobiography of Imam Samudra, mastermind of the 2002 Bali nightclub bombings that killed 202, promotes online credit-card fraud to raise funds. . . . Saudi Arabia launches the Sakinah Campaign, in which Islamic scholars steer religious questioners away from online extremists.

2005 YouTube, launched in February, quickly becomes repository for jihadist video content and commentary. More than 4,000 Web sites connected to terrorist groups are on the Internet.

2006-Present *Governments reauthorize and expand antiterrorism laws; U.K. begins prosecuting those who use the Internet to "incite" others to commit terrorist acts.*

2006 President Bush reauthorizes Patriot Act. . . . U.K. passes Terrorism Act of 2006, outlawing encouragement or glorification of terrorism; civil libertarians raise concerns about free speech. . . . U.S. State Department creates Digital Outreach Team with two Arabic-speaking employees who converse online with critics of U.S. policies.

2007 EU police agency Europol begins "Check the Web" program, in which member states share in monitoring and evaluating terrorists' Web sites. . . . In July, U.K. resident Younis Tsouli pleads guilty to inciting terrorism after he and two associates used stolen credit cards to register Web site domains that promote terrorisim. . . . Samina Malik becomes the first woman convicted of terrorism in the U.K. for having documents that support violent jihad on her computer. A court of appeals later overturns her conviction, questioning her intent to engage in terrorism.

2008 Three important Islamist terrorist discussion forums disappear from the Internet; analysts assume counterterrorism agencies bombarded the sites with denial-of-service attacks. . . . On Nov. 6, Pakistan's president makes cyberterrorism punishable with death or life imprisonment. . . . In its first prosecution for promoting terrorism online, a German court finds Iraqi Kurdish immigrant Ibrahim Rashid guilty of waging a "virtual jihad" for attempting to recruit individuals online to join al Qaeda and participate in jihad.

2009 Canadian resident Saïd Namouh is convicted on Oct. 1 of planning terrorist acts and distributing jihadist propaganda via the Internet. . . . On Oct. 26 Jordanian teenager Hosam Maher Husein Smadi pleads not guilty of plotting to blow up a Dallas skyscraper on Sept. 24. FBI agents had been keeping tabs on Smadi after discovering him on an extremist Web site earlier this year. . . . Researchers are tracking more than 7,000 Web sites connected to terrorist groups and their supporters.

Web offered was immeasurable and recognized by terrorist groups worldwide."[40]

By the end of 1999, nearly all of the 30 organizations designated by the U.S. State Department as foreign terrorist organizations had a presence on the Internet. By 2005, there were more than 40 designated terrorist groups and more than 4,300 Web sites serving them and their supporters. Today, the number of such Web sites exceeds 7,000, according to Weimann, of Haifa University.[41]

Of these groups, Islamic terrorists have perhaps made the most use of the Internet. When al Qaeda suffered defeat in Afghanistan directly after 9/11, its recruiters in Europe "who had previously encouraged others to travel to mujahidin training camps in Afghanistan, Bosnia-Herzegovina and Chechnya began radically changing their message," wrote Kohlmann, of the NEFA Foundation. "Their new philosophy emphasized the individual nature and responsibility of jihad."[42] Recruits did not necessarily have to travel abroad; they could learn what they needed online.

Thus the Internet became a vital means for communication amid a global law enforcement clampdown on suspected terrorists.

Al Qaeda's first official Web site was the brainchild of a senior Saudi operative — and one-time Osama bin Laden bodyguard — Shaykh Youssef al-Ayyiri. The site contained audio and video clips of the al-Qaeda leader, justification for the 9/11 attacks and poetry glorifying the attackers and — on its English version — a message to the American people.[43]

After al-Ayyiri's 2003 death during a clash with Saudi security forces, his top lieutenant, Abdelaziz al-Muqrin, took control. He was a "firm believer in using the Web to disseminate everything from firsthand accounts of terrorist operations to detailed instructions on how to capture or kill Western tourists and diplomats," according to Kohlmann. Before he was killed by Saudi forces in 2004, al-Muqrin created several digital magazines, including *Sawt al-Jihad*, or *The Voice of Jihad.* The author of an article in its inaugural issue told readers, "The blood [of the infidels] is like the blood of a dog and nothing more."[44]

While al Qaeda's Saudi Arabian network pioneered the use of online publications, Kohlmann said, "The modern revolution in the terrorist video market has occurred in the context of the war in Iraq and under the watchful eye of Jordanian national Abu Musab al-Zarqawi." Until his death in 2006, Zarqawi led al Qaeda in Iraq and was known for "his penchant for and glorification of extreme violence — particularly hostage beheadings and suicide bombings," many of them captured on video, including the murder of American civilian contractor Nicholas Berg.[45]

"Images of orange-clad hostages became a headline-news staple around the world — and the full, raw videos of their murders spread rapidly around the Web."[46]

Content on militant Islamist Web sites in Southeast Asia tends to "mimic the contents and features of their Arabic and Middle Eastern online counterparts," according to a study from the Australian Strategic Policy Institute. "Although they aren't yet on par in operational coordination and tradecraft, they are catching up."[47]

Between 2006 and July 2007, extremist content on radical Bahasa Indonesia (the official language of Indonesia) and Malay language Web sites consisted of propaganda from al Qaeda and the Indonesian jihadist group Jemaah Islamiyah. The sites celebrated mujahidin victories, aired local grievances linked to the global jihad and posted highly selective Koranic verses used to justify acts of terror. In August 2007, one of the first postings of instructions on computer hacking appeared, and in the first four months of 2008 the first bomb-making manual, bomb-making video and a password-protected forum emerged.[48] (*See box, p. 134.*)

Not all terrorist organizations use the Internet to showcase violence. Many, such as FARC (Revolutionary Armed Forces of Colombia), focus on human rights and peace. "In contrast to al Qaeda's shadowy, dynamic, versatile and often vicious Web sites," wrote Weimann, "the FARC sites are more 'transparent,' stable and mainly focused on information and publicity."

Established in 1964 as the military wing of the Colombian Communist Party, FARC has been responsible for kidnappings, bombings and hijackings and funds its operations through narcotics trafficking.[49] Yet there are no violent videos of these attacks. Instead, FARC Web sites offer information on the organization's history and laws, its reasons for resistance, offenses perpetrated by the Colombian and U.S. governments, life as a FARC member and women and culture. Weimann called the sophisticated FARC Web sites "an impressive example of media-savvy Internet use by a terrorist group."[50]

From Web 1.0 to 2.0

Terrorist content can now be found on all parts of the Internet, not just on official sites of groups like FARC and al Qaeda and their proxies. Chat rooms, blogs, social

'Terrorists Are Trying to Attract Young Recruits'

An interview with the director of the Dark Web project.

The University of Arizona's Dark Web project, funded by the National Science Foundation, studies international terrorism using automated computer programs. The project has amassed one of the world's largest databases on extremist/ terrorist-generated Internet content. Author Barbara Mantel recently interviewed Hsinchun Chen, the project's director.

CQ: What is the purpose of Dark Web?

HC: We examine who terrorists talk to, what kind of information they disseminate, what kind of new violent ideas they have, what kind of illegal activities they plan to conduct. We're looking at Web sites, forums, chat rooms, blogs, social networking sites, videos and virtual worlds.

CQ: How difficult is it to find terrorist content on the Web?

HC: From Google you can find some, but you won't be able to get into the sites that are more relevant, more intense and more violent.

CQ: So how do sympathizers find these sites?

HC: Typically people are introduced by word of mouth, offline. And there are different degrees of openness on these sites.

CQ: For example?

HC: There are many sites that require an introduction; they may require a password; moderators may also ask a series of questions to see if you are from the region, if you are real and if you are in their targeted audience.

CQ: How does the Dark Web project find these sites?

HC: We have been collaborating for six or seven years with many terrorism study centers all around the world, and they have been monitoring these sites for some time. So they know how to access these Web sites and whether they are legitimate forums. But most of them do not have the ability to collect all the content; they can do manual review and analysis.

So these researchers will give us the URLs of these sites, and they'll give us the user names and passwords they've been using to gain access. Once we get this information, we load it into our computer program, and the computers will spit out every single page of that site and download that into our database.

CQ: How much material are we talking about?

HC: The researchers we work with can analyze maybe hundreds or thousands of pages or messages, but we collect and analyze maybe half a million to 10 million pages easily.

CQ: How do you know that a site is actually linked to a terrorist group or supporter?

HC: Remember we start off with the URLs that terrorism researchers think are important. We also do "crawling" to find new sites. Any Web site will have links to other sites, and by triangulating those links from legitimate sites, we can locate other legitimate sites.

CQ: After finding the content, do you analyze it?

HC: Our claim to fame is analysis. We have techniques that look at social network linkages, that categorize the content into propaganda, training, recruiting, etc., and techniques that determine the sophistication of Web sites. We have a technique that looks at the extent of the violent sentiment in these sites and techniques that can determine authorship.

networking sites and user groups allow conversation and debate among a wide variety of participants.

"Yahoo! has become one of al Qaeda's most significant ideological bases of operations," wrote researchers Rita Katz and Josh Devon in 2003. "Creating a Yahoo! Group is free, quick and extremely easy. . . . Very often, the groups contain the latest links to jihadist Web sites, serving as a jihadist directory."[51] A Yahoo! user group is a hybrid between an electronic mailing list and a discussion forum. Members can receive posted messages and photos through e-mail or view the posts at the group's Web site.

While much of the original content on the terrorist-linked sites was text-based, videos began to play a much larger role after 2003, especially for militant Islamist organizations and their supporters. "Nevertheless, much of this video content remained quite difficult to access for Westerners and others, as it was located on Arabic-only Web sites" that were often frequently changing domain names and were therefore used "only by those who were strongly committed to gaining access," according to a study co-authored by Conway, of Dublin City University.[52]

CQ: None of this is done manually?

HC: Everything I talk about — almost 90 percent — is entirely automated.

CQ: What trends you are noticing?

HC: I'm not a terrorism researcher, but there are trends that we observe on the technology end. Terrorists are trying to attract young recruits, so they like to use discussion forums and YouTube, where the content is more multimedia and more of a two-way conversation. We also see many home-grown groups cropping up all over the world.

CQ: Do you share this information with government agencies?

HC: Many agencies — I cannot name them — and researchers from many countries are using the Dark Web forum portal.

CQ: How does the portal work?

HC: There is a consensus among terrorism researchers that discussion forums are the richest source of content, especially the forums that attract sometimes 50,000 members to 100,000 members. So we have created this portal that contains the contents from close to 20 different, important forums. And these are in English, Arabic and French. The French ones are found in North Africa.

We also embedded a lot of search, translation and analysis mechanisms in the portal. So now any analyst can use the content to see trends. For example, they can see what are the discussions about improvised explosive devices in Afghanistan, or they can look at who are the members that are interested in weapons of mass destruction.

CQ: Are these forums mostly extremist jihadi forums?

HC: Yes, they are. That's what analysts are primarily interested in. We are also creating another portal for multimedia content that will be available in another month or two. That would contain material from YouTube, for instance.

AP Photo/John Miller

Hsinchun Chen oversees the University of Arizona's Dark Web project, which analyzes terrorists' online activities.

CQ: Do you collect information from U.S. extremist sites?

HC: We collect from animal-liberation groups, Aryan Nation and militia groups, but that is just for our research purposes. We don't make it available to outsiders. Government lawyers advise us against giving that kind of information out to them or to the outside world. It's a civil liberty issue.

CQ: Even if that material is open source material, available to anyone who finds their Web site?

HC: Even if it is open source.

But the advent of YouTube in 2005 changed the situation dramatically, Conway wrote, playing an increasing role in distributing terrorist content. Not only did YouTube become an immediate repository for large amounts of jihadist video content, but the social-networking aspects of the site allowed a dialogue between posters and viewers of videos.[53]

Terrorists-linked groups also have used mass e-mailings to reach broad audiences, according to Denning. "The Jihadist Cyber-Attack Brigade, for example, announced in May 2008 they had successfully sent 26,000 e-mails to 'citizens of the Gulf and Arab countries explaining the words of our leader Usama Bin Ladin.'"[54]

Terrorists and Cybercrime

Terrorists increasingly have turned to the Internet to raise funds, often through cybercrime. "We should be extremely concerned about the scope of the credit-card fraud problem involving terrorists," according to Dennis Lormel, a retired special agent in the FBI. Although there is "limited or no empirical data to gauge the extent

Political Change Is Main Attack Motivation

Four out of six types of cyber attacks or threats are politically motivated. Attackers typically use “malware,” or malicious software that spreads viruses, or denial-of-service attacks to disrupt Web sites of individuals, companies, governments and other targets.

Cyber Threat	Motivation	Target	Method
Cyberterror	Political or social change	Innocent victims	Computer-based violence or destruction
Hacktivism*	Political or social change	Decision-makers or innocent victims	Web page defacements or denial of service
Black Hat Hacking**	Ego, personal enmity	Individuals, companies, governments	Malware, viruses, worms or hacking
Cybercrime	Economic gain	Individuals, companies	Malware for fraud or identity theft; denial of service for blackmail
Cyber Espionage	Economic or political gain	Individuals, companies, governments	Range of techniques
Information War	Political or military gain	Infrastructures, information-technology systems and data (private or public)	Range of techniques

** Hacking to promote an activist’s political ideology.*

*** Hacking just for the challenge, bragging rights or due to a personal vendetta.*

Source: Franklin D. Kramer, Stuart H. Starr and Larry Wentz, eds., “Cyber Threats: Defining Terms,” Cyberpower and National Security *(2009)*

of the problem . . . there are compelling signs that an epidemic permeates,” he wrote.[55]

In his jailhouse autobiography, Imam Samudra — convicted of masterminding the 2002 nightclub bombings in Bali, Indonesia, that killed 202 people — includes a rudimentary outline of how to commit online credit-card fraud, or “carding.”

“If you succeed at hacking and get into carding, be ready to make more money within three to six hours than the income of a policeman in six months,” Samudra writes. “But don’t do it just for the sake of money.” Their main duty, he tells readers, is to raise arms against infidels, “especially now the United States and its allies.”[56] Although Samudra’s laptop revealed an attempt at carding, it’s not clear he ever succeeded.

But others have. Younis Tsouli, a young Moroccan immigrant in London who made contact with al Qaeda online, and two associates used computer viruses and stolen credit-card accounts to set up a network of communication forums and Web sites that hosted “everything from tutorials on computer hacking and bomb making to videos of beheadings and suicide bombing attacks in Iraq,” said Lormel.[57]

The three hackers ran up $3.5 million in charges to register more than 180 Web site domains at 95 different Web hosting companies and purchased hundreds of prepaid cellphones and more than 250 airline tickets. They also laundered money through online gaming sites.[58]

Even though both Samudra and Tsouli are in jail, “they left their successful tradecraft on Web pages and in chat rooms for aspiring terrorists to learn and grow from,” noted Lormel.[59]

CURRENT SITUATION

Alternative Voices

Western governments and terrorism experts are concerned that the United States and other nations are not providing a counter message to online militant Islamists.

“The militant Islamist message on the Internet cannot be censored, but it can be challenged,” says Johnny Ryan, a senior researcher at the Institute of International and European Affairs in Dublin, Ireland. But governments and societies, he says, for the most part, have ceded the dialogue in cyberspace to extremists, who are highly skilled at crafting their message.

That message “is mostly emotional,” according to Frank Cilluffo, director of the Homeland Security Policy Institute at The George Washington University in Washington, D.C. It “uses images, visuals and music to tell a powerful story with clear-cut heroes and villains."

Societies interested in countering that message should not shy away from emotion either, he argues. "Who are the victims of al Qaeda?" Cilluffo asks, "and why don't we know their stories?" Western and Arab-Muslim media rarely reveal victims' names unless they are famous or foreign, he points out. Personal stories about victims "from the World Trade Center to the weddings, funerals, schools, mosques and hotels where suicide bombers have brought untold grief to thousands of families, tribes and communities throughout the Muslim world" could be told in online social networks, he suggested, "creating a Facebook of the bereaved that crosses borders and cultures."[60]

Raising doubts is "another powerful rhetorical weapon," says Ryan, who suggests exploiting the chat rooms and discussion forums frequented by prospective militants and sympathizers. Moderate Islamic voices should question the legitimacy of al Qaeda's offensive jihad, disseminate the arguments of Muslim scholars who renounce violence and challenge militant Islamists' version of historical relations between the West and Islam, according to Ryan.[61]

The U.S. Department of State has begun its own modest online effort. In November 2006 it created a Digital Outreach Team with two Arabic-speaking employees. The team now has 10 members who actively engage in conversations on Arabic-, Persian- and Urdu-language Internet sites, including blogs, news sites and discussion forums. Team members identify themselves as State Department employees, but instead of posting dry,

The Top 10 Jihadi Web Forums

The most influential jihadi online forums serve as virtual community centers for al Qaeda and other Islamic extremists, according to Internet Haganah — an online network dedicated to combating global jihad. Jihadi Web addresses, which are often blocked, change frequently.

1 ***al-Faloja***
Highly respected among terrorists; focuses on the Iraq War and the Salafi-jihadi struggle.

2 ***al-Medad***
Was associated with Abu Jihad al-Masri, the al-Qaeda propaganda chief killed in a U.S. missile strike in Pakistan on Oct. 30, 2008; disseminates Salafi-jihadi ideology.

3 ***al-Shouaraa***
Originally named el-Shouraa, it was blocked, but later reemerged with a new name; has North African influences; no longer active.

4 ***Ana al-Muslm***
Very active; was used by al Qaeda to communicate with Abu Musab al-Zarqawi (Osama bin Laden's deputy in Iraq) until he was killed by U.S. forces in 2006.

5 ***al-Ma'ark***
Has been slowly and steadily building an online following in recent years.

6 ***al-Shamukh***
Successor to al-Mohajrun, a militant Islamic organization that was banned in the U.K. in 2005; provides radio broadcasts.

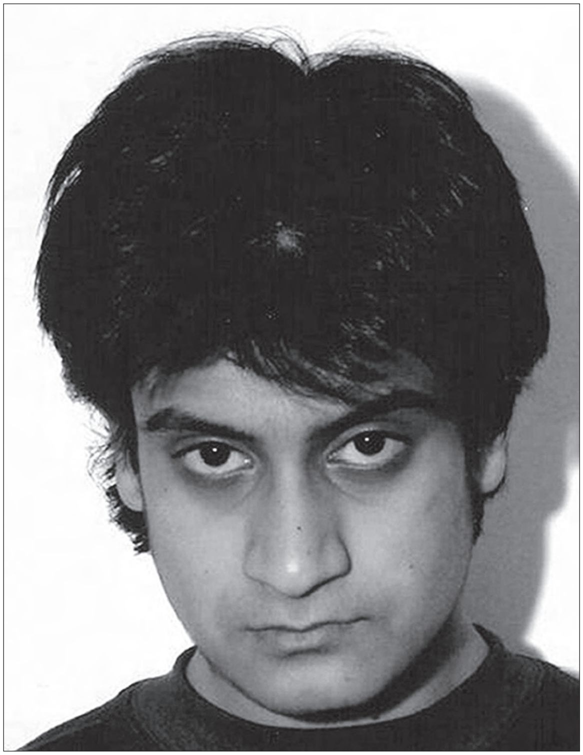
7 ***as-Ansar***
Features English and German invitation-only spin-off sites; a favorite among Western jihadists.

8 ***al-Mujahideen***
Attracts a strong contingent of Hamas supporters, with an overall global jihad perspective; especially focused on electronic jihad.

9 ***al-Hanein***
Has a significant amount of jihadi content tinged by Iraqi, Egyptian and Moroccan nationalism.

10 ***at-Tahaddi***
Sunni jihadist; recruits from Somali, Taliban and other terrorist groups.

Source: "Top Ten List of Jihadi Forums," Internet Haganah, a project of The Society for Internet Research, Aug. 3, 2009, http://internethaganah.com/harchives/006545. html; Jamestown Foundation



AP Photo/West Yorkshire Police/PA Wire

Hamaad Munshi — a British national convicted in 2008 of possessing materials likely to be used for terrorism — was 16 when he was arrested after participating in an online British extremist group. The trial revealed that Munshi had downloaded details on how to make napalm and grenades and wished to become a martyr by fighting abroad.

policy pronouncements they create "engaging, informal personas for [their] online discussions." The team's mission is "to explain U.S. foreign policy and to counter misinformation," according to the State Department.[62]

No one knows the full impact of the team's efforts, but the project has come in for criticism. "They should be larger," says Matt Armstrong, an analyst and government advisor who writes a blog on public diplomacy at mountainrunner.us, "and they should be coordinated to a much greater degree with the production side of the State Department." The team's Internet conversations should directly shape a post on the State Department Web site or on its radio program, he says.

But Duncan MacInnes, principal deputy coordinator at the State Department's Bureau of International Information Programs, says the scale of the Digital Outreach Team is about right, although it could use one or two more Persian speakers and possibly expand into more languages. "Having too many people blogging in a fairly small blogosphere would raise our profile, and we felt [it] would create a reaction against us. You don't want to overdo it." Also, he says, the team does not work in isolation. It writes a biweekly report about the issues, concerns and misunderstandings members encounter online, which goes to hundreds of people inside the State Department.

Others question whether the government should be the one to hold this dialogue. "The state is not in a position to be the primary actor here because it lacks credibility in online forums," says Ryan.

"The best approach is to provide young people with the information and the intellectual tools to challenge this material themselves on various Web forums," says Bergin, of the Australian Strategic Policy Institute. "It's got to be provided by stakeholders in the Muslim community themselves, from community workers, religious figures and parents."

The Sakinah Campaign

Many terrorism analysts cite Saudi Arabia's Sakinah Campaign as a model program. Internet use in the kingdom has grown rapidly since access first became available there 10 years ago. Since 2000, the kingdom's total number of Internet users has risen from roughly 200,000 to more than 7 million today, out of an overall population of nearly 29 million.[63]

Meanwhile, extremist Web sites in the kingdom have multiplied from 15 sites in 1998 to several thousand today, even though the Saudi government controls Internet access and blocks sites featuring gambling, pornography and drug and alcohol use, according to Christopher Boucek, a researcher at the Carnegie Endowment for International Peace. Extremist sites "often appear faster than they can be identified and blocked," said Boucek.[64]

Responding to that trend, the Sakinah Campaign since 2004 has used volunteer Islamic scholars "to interact online with individuals looking for religious knowledge, with the aim of steering them away from extremist sources." These scholars have "highly developed understandings of extremist ideologies, including the religious interpretations used

AT ISSUE

Is cyberterrorism a significant global threat?

YES

Mohd Noor Amin
Chairman, International Multilateral Partnership Against Cyber Threats Selangor, Malaysia

Written for *CQ Global Researcher*, November 2009

Alarm bells on cyberterrorism have been sounding for more than a decade, and yet, hacktivism aside, the world still has not witnessed a devastating cyber attack on critical infrastructure. Nothing has occurred that caused massive damage, injuries and fatalities resulting in widespread chaos, fear and panic. Does that mean the warnings were exaggerated?

On the contrary, the convergence of impassioned politics, hacktivism trends and extremists' growing technological sophistication suggests that the threat of cyberterrorism remains significant — if not more urgent — today. Although hacktivists and terrorists have not yet successfully collaborated to bring a country to its knees, there is already significant overlap between them. Computer-savvy extremists have been sharpening their skills by defacing and hacking into Web sites and training others to do so online. Given the public ambitions of groups like al Qaeda to launch cyber attacks, it would be folly to ignore the threat of a major cyber assault if highly skilled hackers and terrorists did conspire to brew a perfect storm.

Experts are particularly concerned that terrorists could learn how to deliver a simultaneous one-two blow: executing a mass, physical attack while incapacitating the emergency services or electricity grids to neutralize rescue efforts. The scenario may not be so far-fetched, judging from past cyber attacks or attempts, although a certain level of technical skill and access would be needed to paralyze part of a nation's critical infrastructure. However, as shown by an oft-cited 2000 incident in Australia, a single, disgruntled former employee hacked into a wastewater management facility's computer system and released hundreds of thousands of gallons of raw sewage onto Sunshine Coast resort grounds and a canal.

Vital industrial facilities are not impenetrable to cyber attacks and, if left inadequately secured, terrorists and hackers could wreak havoc. Similarly, the 2008 cyber attacks that caused multicity power outages around the world underscore the vulnerabilities of public utilities, particularly as these systems become connected to open networks to boost economies of scale.

If this past decade of terrorist attacks has demonstrated the high literacy level, technological capability and zeal of terrorists, the next generation of terrorists growing up in an increasingly digitized and connected world may hold even greater potential for cyberterrorism. After all, if it is possible to effect visibly spectacular, catastrophic destruction from afar and still remain anonymous, why not carry it out?

NO

Tim Stevens
Associate, Centre for Science and Security Studies, King's College London

Written for *CQ Global Researcher*, November 2009

Cyberterrorism is the threat and reality of unlawful attacks against computer networks and data by an individual or a non-governmental group to further a political agenda. Such attacks can cause casualties and deaths through spectacular incidents, such as plane crashes or industrial explosions, or secondary consequences, such as crippled economies or disrupted emergency services.

We have seen many attempts to disrupt the online assets of governments, industry and individuals, but these have mercifully not yet caused the mass casualties predicted by the term "cyberterrorism." The assumption that terrorists might use cyberspace in such attacks is not in question, but the potential threat that cyberterrorism poses is accorded disproportionate weight in some circles.

Cyberterrorism resulting in civilian deaths is certainly one possible outcome of the convergence of technology and political aggression. That it has not happened yet is a function of two factors. First, the ongoing vigilance and operational sophistication of national security agencies have ensured that critical infrastructure systems have remained largely unbreached and secure. And second, like all self-styled revolutionaries, terrorists talk a good talk.

Although a terrorist group might possess both the intent and the skill-sets — either in-house, or "rented" — there is little evidence yet that any group has harnessed both to serious effect. Most attacks characterized as "cyberterrorism" so far have amounted to mere annoyances, such as Web site defacements, service disruptions and low-level cyber "skirmishing" — nonviolent responses to political situations, rather than actions aimed at reaping notoriety in flesh and blood.

It would be foolish, however, to dismiss the threat of cyberterrorism. It would also be disingenuous to overstate it. Western governments are making strides towards comprehensive cyber security strategies that encompass a wide range of possible scenarios, while trying to overcome agency jurisdictional issues, private-sector wariness and the fact that civilian computer systems are now seen as "strategic national assets."

As it becomes harder to understand the complexities of network traffic, identify attack vectors, attribute responsibility and react accordingly, we must pursue integrated national and international strategies that criminalize the sorts of offensive attacks that might constitute cyberterrorism. But designating the attacks as terrorism is a taxonomic firewall we should avoid.

to justify violence and terrorism," according to Boucek.[65] The campaign is officially an independent, nongovernmental project, even though several government ministries encourage and support it.

According to Abdullah Ansary, a lawyer and former lecturer at King Abdul-Aziz University in Saudi Arabia, al Qaeda has issued several statements over the Internet cautioning their followers not to engage in dialogues with members of the Sakinah Campaign, a sign that the campaign is having an impact on al Qaeda's membership.[66] The campaign itself periodically releases the number of people it says it has turned away from extremism. In January 2008, it announced it had "convinced some 877 individuals (722 male and 155 female) to reject their radical ideology across more than 1,500 extremists Web sites."[67]

But in 2007, after the government arrested members of seven terrorist cells operating in the kingdom, several columnists complained that the Sakinah Campaign and other government supported programs trying to reform extremists were ineffective and not getting to the root of the problem. According to translations from the Middle East Media Research Institute, columnist Abdallah bin Bajad Al-'Utaibi wrote in the Saudi daily *Al-Riyadh*: "There are schoolteachers, imams in the mosques, preachers and jurisprudents who do nothing but spread hatred and *takfir** in our society. They should be prosecuted for their actions, which lay down the foundations for terrorism."[68]

Ansary said the government must make wider reforms if it wants to prevent young people from turning to extremism. The government must "speed up the process of political reform in the country, widening popular participation in the political process, improving communication channels of both the government and the public, creating effective communication among branches of government, continuing the efforts in overhauling the Saudi educational system and boosting the role of women in the society."[69]

In late 2006, the Sakinah Campaign expanded its role and created its own Web site designed to "serve as a central location for people to turn to online with questions about Islam."[70]

Government-funded Sites

Similar Web sites have been set up in other countries to offer alternative messages to terrorist propaganda.

The Islamic Religious Council of Singapore — the country's supreme Islamic authority, whose members are appointed by the country's president — has several interactive Web sites to counter extremist strands of Islam. The sites feature articles, blogs and documentary videos targeted at young people and host an online forum where religious scholars answer questions about Islam. One site specifically challenges the ideology of Jemaah Islamiyah, the jihadist group responsible for the deadly 2002 nightclub bombing in Bali and the July 2009 bombings of the Marriott and Ritz Carlton hotels in Jakarta. The organization wants to establish a pan-Islamic theocratic state across much of Southeast Asia.[71]

But the effectiveness of such sites is difficult to gauge. "To a certain extent it is helping to drown out extremist voices online," says Osman, of Nanyang Technological University in Singapore, "but for those who are actively seeking extremist ideology, these kinds of Web sites don't appeal to them."

A similar project in the United Kingdom also meets with skepticism. On its Web site, the Radical Middle Way calls itself "a revolutionary grassroots initiative aimed at articulating a relevant mainstream understanding of Islam that is dynamic, proactive and relevant to young British Muslims."[72] It rejects all forms of terrorism, and its site has blogs, discussions, videos, news and a schedule of its events in the U.K. Its two dozen supporters and partners are mostly Muslim organizations as well as the British Home Office, which oversees immigration, passports, drug policy and counterterrorism, among other things.

"We are arguing that this is not money well spent," says Neumann of King's College. "The kind of money the government is putting into the Web site is enormous, and the site doesn't attract that much traffic."

The government money has also caused at least some young people to question the group's credibility. One blogger called the group "the radical wrong way" and wrote that "because the funding source is so well known, large segments of alienated British Muslims will not have anything to do with this group. . . . If anything, such tactics will lead to even further alienation of young British Muslims — who will rightly point out that this kind of U.S./U.K.-funded version of Islam is just another strategy in the ongoing war on Islam."[73]

Neumann and Bergin recommend instead that governments give out many small grants to different Muslim

* *Takfir* is the act of identifying someone as an unbeliever.

organizations with ideas for Web sites and see if any can grow to significance without dependence on government funds.

In the end, individual governments' direct role in providing an online alternative narrative to terrorist ideology may, out of necessity, be quite small because of the credibility issue, say analysts. Instead, they say, governments could fund Internet literacy programs that discuss hate propaganda, adjust school curriculums to include greater discussion of Islam and the West and encourage moderate Muslim voices to take to the Web. Cilluffo, of the Homeland Security Policy Institute, said the United Nations could lead the way, sponsoring a network of Web sites, publications and television programming.

"The United Nations can and should play a significant role," Cilluffo said, "bringing together victims to help meet their material needs and raising awareness by providing platforms through which to share their stories."[74]

OUTLOOK

Pooling Resources

Web sites that promote terrorism are here to stay, although governments and Internet companies will occasionally shut one down if it violates the law or a terms-of-service agreement. Such decisions can only be reached after prolonged monitoring and "must weigh the intelligence value against the security risk posed by the Web site," says Jordanian terrorism expert Bakier.

But monitoring the thousands of Web sites, discussion forums, chat rooms, blogs and other open sources of the Web requires trained personnel with expertise in the languages, cultures, belief systems, political grievances and organizational structures of the terrorist groups online. Because such personnel are scarce, most experts agree that nations should pool their resources. "It is hardly possible for one individual member state to cover all suspicious terrorism-related activities on the Internet," according to a European Union (EU) report.[75]

Good intentions aren't enough. "There are lots of conferences, lots of declarations, lots of papers, but in reality, you have different counterterrorism agencies not sharing information, competing, afraid of each other, sometimes in the same state and also across borders," says Haifa University's Weimann.

AFP/Getty Images/Torsten Blackwood

Above, an Internet café in Sydney. Many Australians oppose government plans to build what critics call the Great Aussie Firewall — a mandatory Internet filter that would block at least 1,300 Web sites prohibited by the government.

Europol, the EU police agency, began a program in 2007 called Check the Web, which encourages member nations to share in monitoring and evaluating open sources on the Web that promote or support terrorism. The online portal allows member nations to post contact information for monitoring experts; links to Web sites they are monitoring; announcements by the terrorist organizations they are tracking; evaluations of the sites being monitored and additional information like the possibility of legal action against a Web site.

Weimann, who calls the program a "very good idea and very important," says he cannot directly evaluate its progress, since access is restricted to a handful of counterterrorism officials in each member nation. But he does speak to counterterrorism experts at workshops and conferences, where he hears that "international cooperation — especially in Europe — is more theoretical than practical."

When asked if barriers exist to such cooperation, Dublin City University's Conway says, "Emphatically, yes! These range from protection-of-institutional-turf issues — on both a national and EU-wide basis — to potential legal constraints." For instance, she says, some member states' police are unsure whether or not they need a court order to monitor and participate in a Web forum without identifying themselves. Others disagree about the definition of a terrorist and what kinds of sites should be watched.

These barriers may not be the program's only problem. "It might be a disadvantage that so far just EU countries participate," according to Katharina von Knop, a professor of international politics at the University of the Armed Forces, in Munich, Germany, thus limiting the expertise available.[76]

NOTES

1. Abdul Hameed Bakier, "An Online Terrorist Training Manual — Part One: Creating a Terrorist Cell," Terrorism Focus, vol. 5, no. 13, The Jamestown Foundation, April 1, 2008. The ek-Is.org Web site has also gone under various other names, including ekhlass.org.
2. *Ibid.*
3. Bakier, *op. cit.*, "Part Two: Assassinations and Robberies," vol. 5, no. 14, April 9, 2008.
4. Bakier, *op. cit.*, "Part Three: Striking U.S. Embassies," vol. 5, no. 15, April 16, 2008.
5. Gabriel Weimann, *Terror on the Internet*, United States Institute of Peace Press (2006), p. 51.
6. *Ibid.*, p. 30.
7. University of Arizona, "Artificial Intelligence Lab Dark Web Project," www.icadl.org/research/terror/.
8. "The 9/11 Commission Report," www.9-11commission.gov/report/index.htm.
9. Anne Stenersen, "The Internet: A virtual training camp?" Norwegian Defense Research Establishment, Oct. 26, 2007, p. 3, www.mil.no/multimedia/archive/00101/Anne_Stenersen_Manu_101280a.pdf.
10. Dorothy Denning, "Terror's Web: How the Internet Is Transforming Terrorism," Handbook on Internet Crime, 2009, p. 19, http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf.
11. *Ibid.*, p. 4.
12. "Violent Islamic Extremism, the Internet, and the Homegrown Terrorist Threat," U.S. Senate Committee on Homeland Security and Governmental Affairs, May 8, 2008, pp. 2, 13, http://hsgac.senate.gov/public/_files/IslamistReport.pdf.
13. "Safeguarding Online: Explaining the Risk Posed by Violent Extremism," Office of Security and Counter Terrorism, Home Office, Aug. 10, 2009, p. 2, http://security.homeoffice.gov.uk/news-publications/publication-search/general/Officers-esafety-leaflet-v5.pdf?view=Binary.
14. *Ibid.*
15. Peter Neumann and Tim Stevens, "Countering Online Radicalisation: A Strategy for Action," The International Centre for the Study of Radicalisation and Political Violence, Kings College London, 2009, p. 14, www.icsr.info/news/attachments/1236768445ICSROnlineRadicalisationReport.pdf.
16. Clodagh Hartley, "Govt Can't Stop 'Web of Terror,'" *The Sun* (England), March 20, 2009, p. 2.
17. "Interview given by Mme. Michèle Alliot-Marie, French Minister of the Interior, to Le Figaro," French Embassy, Feb 1, 2008, www.ambafrance-uk.org/Michele-Alliot-Marie-on-combating.html.
18. Greg Goth, "Terror on the Internet: A Complex Issue, and Getting Harder," IEEE Computer Society, March 2008, www2.computer.org/portal/web/csdl/doi/10.1109/MDSO.2008.11.
19. Howard Altman, "Al Qaeda's Web Revival," *The Daily Beast*, Oct. 2, 2009, www.thedailybeast.com/blogs-and-stories/2009-10-02/is-this-al-qaedas-website.
20. Gregory McNeal, "Cyber Embargo: Countering the Internet Jihad," *Case Western Reserve Journal of International Law*, vol. 39, no. 3, 2007-08, p. 792.
21. *Brandenburg v. Ohio*, www.oyez.org/cases/1960-1969/1968/1968_492/.
22. "Safeguarding Online: Explaining the Risk Posed by Violent Extremism," *op. cit.*, p. 3.
23. Elizabeth Renieris, "Combating Incitement to Terrorism on the Internet: Comparative Approaches in the United States and the United Kingdom and the Need for an International Solution," *Vanderbilt Journal of Entertainment and Technology Law*, vol. 11:3:673, 2009, pp. 687-688.
24. Fergus Watts, "Caught out by net plan," *Herald Sun* (Australia), Dec. 29, 2008, p. 20, www.heraldsun.com.au/opinion/caught-out-by-net-plan/story-6frfifo-1111118423939.
25. Weimann, *op. cit.*, p. 180.

26. "Jordanian accused in Dallas bomb plot goes to court," CNN, Sept. 25, 2009, www.cnn.com/2009/CRIME/09/25/texas.terror.arrest/index.html.
27. http://smallbusiness.yahoo.com/tos/tos.php.
28. Neumann and Stevens, *op. cit.*, p. 32.
29. Maura Conway, "Terrorism & Internet Governance: Core Issues," U.N. Institute for Disarmament Research, 2007, p.11. www.unidir.org/pdf/articles/pdf-art2644.pdf.
30. Isambard Wilkinson, "Pakistan sets death penalty for 'cyber terrorism,' " *Telegraph.co.uk*, Nov 7, 2008, www.telegraph.co.uk/news/worldnews/asia/pakistan/3392216/Pakistan-sets-death-penalty-for-cyber-terrorism.html.
31. "Cyber attacks and cyber terrorism are the new threats," *India eNews*, March 26, 2009, www.indiaenews.com/print/?id=187451.
32. Linda McGlasson, "ATM Fraud Linked in RBS WorldPay Card Breach," Bank info Security, Feb. 5, 2009, www.bankinfosecurity.com/articles.php?art_id=1197.
33. Dorothy Denning, "A View of Cyberterrorism Five Years Later," 2007, pp. 2–3, http://faculty.nps.edu/dedennin/publications/Denning-TerrorsWeb.pdf.
34. Steven Bucci, "The Confluence of Cyber-Crime and Terrorism," Heritage Foundation, June 15, 2009, p. 6, www.heritage.org/Research/NationalSecurity/upload/hl_1123.pdf.
35. *Ibid.*, p. 5.
36. *Ibid.*, p. 6.
37. Dorothy Denning, *op. cit.*, p. 15.
38. *Ibid.*
39. Denning, "Terror's Web: How the Internet is Transforming Terrorism," *op. cit.*, p. 2.
40. *Ibid.*
41. Weimann, *op. cit.*, p. 15.
42. Evan Kohlmann, " 'Homegrown' Terrorists: Theory and Cases in the War on Terror's Newest Front," *The Annals of the American Academy of Political and Social Science*, July 2008; 618; 95. p. 95.
43. Denning, "Terror's Web: How the Internet is Transforming Terrorism," *op. cit.*, p. 3.
44. Kohlmann, *op. cit.*, p. 101.
45. *Ibid.*
46. David Talbot, "Terror's Server," *Technology Review.com*, Jan. 27, 2005, www.militantislammonitor.org/article/id/404.
47. Anthony Bergin, *et al.*, "Countering Internet Radicalisation in Southeast Asia," The Australian Strategic Policy Institute Special Report, March 2009, p. 5.
48. *Ibid.*, p. 6.
49. Weimann, *op. cit.*, pp. 75-76.
50. Weimann, *op. cit.*, p. 75.
51. Rita Katz and Josh Devon, "WWW.Jihad.com," *National Review Online*, July 14, 2003, http://nationalreview.com/comment/comment-katz-devon071403.asp.
52. Maura Conway and Lisa McInerney, "Jihadi Video & Auto-Radicalisation: Evidence from an Exploratory YouTube Study," 2008, p. 1, http://doras.dcu.ie/2253/2/youtube_2008.pdf.
53. *Ibid.*, p. 2.
54. Denning, "Terror's Web: How the Internet is Transforming Terrorism," *op. cit.*, p. 5.
55. Dennis Lormel, "Terrorists and Credit Card Fraud . . . A Quiet Epidemic," Counterterrorism Blog, Feb. 28, 2008, http://counterterrorismblog.org/2008/02/terrorists_and_credit_card_fra.php.
56. Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace," *The Washington Post*, Dec. 14, 2004, p. A19, www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html.
57. Lormel, *op. cit.*
58. Dennis Lormel, "Credit Cards and Terrorists," Counterterrorism Blog, Jan. 16, 2008, http://counterterrorismblog.org/2008/01/credit_cards_and_terrorists.php.
59. Dennis Lormel, "Terrorists and Credit Card Fraud . . . ," *op. cit.*
60. Frank Cilluffo and Daniel Kimmage, "How to Beat al Qaeda at Its Own Game," *Foreign Policy*, April

2009, www.foreignpolicy.com/story/cms.php?story_id=4820.

61. Johnny Ryan, "EU must take its anti-terrorism fight to the Internet," *Europe's World*, Summer 2007, www.europesworld.org/EWSettings/Article/tabid/191/ArticleType/ArticleView/ArticleID/21068/Default.aspx.
62. Digital Outreach Team, U.S. Department of State, www.state.gov/documents/organization/116709.pdf.
63. "Middle East Internet Usage and Population Statistics," *Internet World Stats*, www.internetworldstats.com/stats5.htm.
64. Christopher Boucek, "The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia," *CTC Sentinel*, August 2008, p. 2, www.carnegieendowment.org/files/CTCSentinel_Vol1Iss9.pdf.
65. *Ibid.*, p. 1.
66. Abdullah Ansary, "Combating Extremism: A brief overview of Saudi Arabia's approach," *Middle East Policy*, Summer 2008, vol. 15, no. 2, p. 111.
67. *Ibid.*
68. Y. Admon and M. Feki, "Saudi Press Reactions to the Arrest of Seven Terrorist Cells in Saudi Arabia," Inquiry and Analysis, no. 354, MEMRI, May 18, 2007.
69. Ansary, *op. cit.*, p. 111.
70. Boucek, *op. cit.*, p. 3.
71. Bergin, *op. cit.*, p. 19.
72. www.radicalmiddleway.co.uk.
73. "A radical wrong way," Progressive Muslims: Friends of Imperialism and Neocolonialism, Oct. 31, 2006, http://pmunadebate.blogspot.com/2006/10/radical-wrong-way.html.
74. Cilluffo and Kimmage, *op. cit.*
75. "Council Conclusions on Cooperation to Combat Terrorist Use of the Internet ("Check the Web")," Council of the European Union, May 16, 2007, p. 3, http://register.consilium.europa.eu/pdf/en/07/st08/st08457-re03.en07.pdf.
76. Katharina von Knop, "Institutionalization of a Web-Focused, Multinational Counter-Terrorism Campaign," *Responses to Cyber Terrorism* (2008), p. 14.

BIBLIOGRAPHY

Books

Jewkes, Yvonne, and Majid Yar, eds., *The Handbook on Internet Crime*, *Willan Publishing*, 2009.
British criminology professors have compiled essays by leading scholars on issues and debates surrounding Internet-related crime, deviance, policing, law and regulation in the 21st century.

Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security*, *Potomac Books*, 2009.
Experts write about cyber power and its strategic implications for national security, including an assessment of the likelihood of cyberterrorism.

Sageman, Marc, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, *University of Pennsylvania Press*, 2008.
A senior fellow at the Center on Terrorism, Counter-Terrorism, and Homeland Security in Philadelphia examines the impact of the Internet on global terrorism, including its role in radicalization, and strategies to combat terrorism in the Internet age.

Weimann, Gabriel, *Terror on the Internet*, *United States Institute of Peace Press, 2006.*
A professor of communication at Haifa University in Israel explores how terrorist organizations exploit the Internet to raise funds, recruit members, plan attacks and spread their message.

Articles

Boucek, Christopher, "The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia," *CTC Sentinel*, August 2008.
Saudi Arabia enlists religious scholars to engage in dialogue on the Internet with individuals seeking out religious knowledge in order to steer them away from extremist beliefs.

Cilluffo, Frank, and Daniel Kimmage, "How to Beat al Qaeda at Its Own Game," *Foreign Policy,* April 2009, www.foreignpolicy.com.

Two American terrorism experts recommend using Web sites, chat rooms, social networking sites, broadcasting and print to tell the stories of Muslim victims of militant Islamist terror attacks.

Goth, Greg, "Terror on the Internet: A Complex Issue, and Getting Harder," *IEEE Distributed Systems Online*, vol. 9, no. 3, 2008.
Counterterrorism agencies cringe when posturing by politicians leads to the dismantling of terrorist Web sites they've been monitoring.

Labi, Nadya, "Jihad 2.0," *The Atlantic Monthly*, July/August, 2006.
With the loss of training camps in Afghanistan, terrorists turned to the Internet to find and train recruits.

Talbot, David, "Terror's Server — How radical Islamists use Internet fraud to finance terrorism and exploit the Internet for Jihad propaganda and recruitment," *Technology Review.com*, Jan. 27, 2008.
Terrorists use the Internet for fundraising, propaganda and recruitment, but government and the Internet industry responses are limited by law and technology.

Reports and Studies

Bergin, Anthony, *et al.*, "Countering Internet Radicalisation in Southeast Asia," Australian Strategic Policy Institute, March 2009.
The director of research at the institute traces the evolution of extremist and terrorist-linked content from static Web sites to the more dynamic and interactive parts of the Internet.

Boyne, Shawn Marie, "The Criminalization of Speech in an Age of Terror," Indiana University School of Law-Indianapolis, working paper, June 12, 2009.
A law professor compares prosecution of incitement to terror in Germany, the U.K. and the United States.

Conway, Maura, "Terrorism & Internet Governance: Core Issues," *Disarmament Forum*, 2007.
A terrorism expert at Dublin City University in Ireland explores the difficulties of Internet governance in light of terrorists' growing use of the medium.

Denning, Dorothy, "Terror's Web: How the Internet is Transforming Terrorism," *Naval Postgraduate School*, 2009.
A professor of conflict and cyberspace discusses the implications of shutting sites down versus continuing to monitor sites or encouraging moderate voices to engage in dialogue online with terrorist sympathizers.

Neumann, Peter R., and Tim Stevens, "Countering Online Radicalisation: A Strategy for Action," *The International Centre for the Study of Radicalisation and Political Violence*, 2009.
Shutting down terrorist sites on the Internet is expensive and counterproductive, according to the authors.

Renieris, Elizabeth, "Combating Incitement to Terrorism on the Internet," *Vanderbilt Journal of Entertainment and Technology Law*, vol. 11:3:673, 2009.
The author compares U.S. and U.K. laws used to prosecute incitement to terrorism on the Internet.