Terror on the Internet: A Complex Issue, and Getting Harder
Greg Goth

The fight against terror on the World Wide Web, chat rooms, and forums tends to take a maddeningly circular route. Politicians demand a crackdown on the terrorist presence on the Web, calling on ISPs to develop new technologies that will block access to terrorist sites or to detect their origin and shut them down.

Just as quickly, the sites’ operators relaunch from another host. Courts have found numerous efforts to thwart terror to be an abridgment of users’ rights of free speech; white-hat security analysts cringe when the political posturing leads to dismantling sites they’ve been surreptitiously monitoring.

In the past two months, the United Kingdom has become the latest microcosm illustrating the dizzying complexity governments face as they attempt to balance stifling terror on the Internet with free speech and information access.

Politicians want action, experts urge caution

In a speech delivered at the First International Conference on Radicalization and Political Violence, held in London on 17 and 18 January, Home Secretary Jacqui Smith called for the ISP community to begin treating terrorist sites like child sexual abuse sites (http://press.homeoffice.gov.uk/Speeches/sp-hs-terrorism-keynote-jan-08). “The Internet is not a no-go area for government,” Smith said as she announced an effort to take terror off the World Wide Web.

“In the next few weeks, I will be talking to industry, and critically those in the community, about how best to do this—and how best to identify material that is drawing vulnerable young people into violent extremism. Where there is illegal material on the Net, I want it removed.”

Smith’s comments drew some puzzlement and skepticism from UK technology-policy observers. ISPs are already mandated to take down jihadi sites when informed of their existence by recognized authorities.

“Essentially, people don’t understand what she’s proposing,” says Richard Clayton, a Cambridge-based computer policy researcher and treasurer of the Foundation for Information Policy Research (FIPR; www.fipr.org), a leading UK Internet policy think tank. “She's not the first person to do this.”

Indeed, politicians around the world call at regular intervals for terrorist websites to be removed from their host sites’ servers or for search engines to block access to them. They also call for laws that would make posting instructions on how to kill or maim people or destroy property punishable by law. Franco Frattini, the European Commission’s Vice President for Freedom, Justice, and Security, called for a prohibition on websites that post bomb-making instructions in September 2007 (http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/07/505&format=HTML&aged=0&language=EN&uiLanguage=en). And just as quickly, he rushed to announce that in doing so he was not trying to impinge on freedom of speech or information access or to inhibit law enforcement agencies from monitoring sites.
"I therefore do not envisage at all limiting our citizens’ capacity of web research,” he said (http://ec.europa.eu/commission_barroso/frattini/news/archives_2007_en.htm#september). "The decision to block a website may be taken where appropriate only when the site has illicit content whose knowledge can run counter to public security—for instance, bomb making. Sometimes, however, law enforcement authorities may decide to keep websites deliberately active for investigating reasons.”

However disarming Frattini might have intended his disclaimer to be, technology policy scholars say such sentiments are usually counterproductive and simplistic. Arguments against information-limiting proposals like Smith’s and Frattini’s tend to run along both technological and philosophical lines.

“Those who think that we can stop online terrorism by removal of websites are either naive or ignorant about cyberspace and its limitations for interference,” says Gabriel Weimann, professor of communication at Haifa University in Israel and author of Terrorism on the Internet (http://bookstore.usip.org/books/BookDetail.aspx?productID=134280). “As a short answer, there is a need for strategy and not tactics, there is a need for a multimeasured approach, and not just “Let’s kill those websites.’ They reemerge within days or even hours.”

Who will decide? Law enforcement, ISPs, or courts?

Blocking websites also brings into play the incredibly labyrinthine arguments around just what is terror-inducing material. For example, a website that trumpets itself as a holy warriors’ resource, complete with instructions on bomb-making, might easily be called a terrorist site and treated as such under law. However, what actions could—or should—an ISP take on an arborists’ informational site that includes instructions on how to make a stump-blowing charge of black powder? Or is that arborists’ site a front for a terror organization?

FIPR’s Clayton says the analogous approach with child abuse sites would probably call for some sort of monitoring organization to receive reports of possible terrorist-linked sites. The volunteer organization charged with this task under the UK’s child abuse statutes is the Internet Watch Foundation (www.iwf.org.uk). The IWF is funded by the EU and what it calls the “wider online industry.” It also claims that because of its role, "less than 1 percent of potentially illegal content has apparently been hosted in the UK since 2003, down from 18 percent in 1997.”

In principle, Clayton says, it’s easy to add sites to these lists for terror websites, but there isn’t a body that will make a list of them. “And it’s difficult to make a list,” he says. “Are you going to put al-Jazeera on the list because they have a video of someone getting his head chopped off?”

Clayton believes that the British government will take an informal route to get the UK’s ISPs to crack down on terrorist sites.

"In the wonderful British way in which we do things, the CEOs of the major ISPs will be invited to meet, probably with the Prime Minister, and be encouraged to do something about that.”

However, Clayton says, exactly what form that encouragement turns out to be might have little effect on users’ rights under the law. On 13 February, just 27 days after Home Secretary Smith’s speech, the British Appeal Court overturned the convictions of five young men who had been charged with downloading and sharing jihadi materials over the Internet (http://news.bbc.co.uk/2/hi/uk_news/7242724.stm). The material included ideological propaganda as well as communications among the appellants and with others. The prosecution alleged the data showed a settled plan under which the appellants would travel to Pakistan to receive training and thereafter commit a terrorist act or acts in Afghanistan. The appeal court, however, decided that the communications between the young men were not detailed enough in concrete plans to fight for jihadi forces in Afghanistan to uphold the convictions. The lower court found the men guilty under Section 57 of the UK’s Terror Act of 2000 (www.opsi.gov.uk/acts/acts2000/ukpga_20000011_en_6#pt6-pb1-l1g57), which states, “A person commits an offence if he possesses an article in circumstances which give rise to a reasonable
suspicion that his possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism."

The appeal court’s decision will only further confuse the issue, Clayton says. "Possession of this stuff is not inherently illegal, and so ISPs are being invited to block stuff because people don’t like it. That will get people a bit twitchy."

US prosecutors trying to toughen the parameters of what constitutes illegal support of terrorist websites have also run into resistance. In one high-profile case, University of Idaho graduate student Sami Omar Al-Hussayen was acquitted of three counts of using his position as a volunteer webmaster of controversial websites to materially aid terror groups (www.eff.org/press/archives/2004/06/10-0). Al-Hussayen’s case was viewed as a vital test of First Amendment rights by free speech advocates such as the Electronic Frontier Foundation.

“I think that both the Home Secretary and Mr. Frattini are talking about aspirations they have, rather than things they could necessarily pass laws about or manage to get the detail pinned down sufficiently to get a law or, alternatively, [things that are] technologically possible,” Clayton says.

Haifa scholar Weimann agrees that the legal vagaries surrounding the issue contribute to the lack of real multilateral agreement on combating online terror.

“There is a lot of interstate dialogue, but it is more talking than doing,” Weimann says. "There is also an interest in developing international forces to combat online terrorism, but not much is actually done."

The Dark Web

As politicians and courts wrangle over the details of what constitutes a terror site and who might legitimately be called a terrorist, the technological battle over terrorists’ use of the Internet has recently taken a more granular turn. ISPs have developed numerous filtering and blocking technologies for websites belonging to a wide variety of criminal elements beyond terrorist organizations, but the site operators have found ways around them. Now jihadists are improving their own black-hat capabilities. In mid-January, the Mujahideen Secrets encryption tool was released. Independent security analyst Dancho Danchev studied the tool and blogged about some of its new features (http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html), including tools that could advance the goal of pasting encrypted messages in web pages instead of in e-mail.

Government-led technological efforts to combat terror on the Web range from working with independent groups that compile and analyze the content from global terror sites to developing deep analytic technologies such as web spiders that can analyze connections between jihadi websites, messages, and forum postings to creating white-hat viruses and malware meant to cripple or compromise jihadi sites. For example, Dark Web is a US National Science Foundation-funded project at the University of Arizona, which develops analytic technologies (www.nsf.gov/news/news_summ.jsp?cntn_id=110040). One Dark Web team studied online stories and videos designed to help train terrorists in how to build improvised explosive devices. According to the NSF, understanding what information is being spread about IED methods and where in the world it’s being downloaded can improve countermeasures that are developed to thwart them.

IPR’s Clayton says the chest-thumping to remove terror sites actually hampers efforts such as Dark Web.
"The funny thing is that so many of the real Al Qaeda websites are hosted in the US," he says. "One simple reason is it’s one of the cheaper places to host. They circulate via mailing lists and these sort of out of bounds methods where they can be found. They’re all in Arabic. Not many westerners know Arabic, and everything’s fine until some journalist figures out where the website is.”

The result of this scenario, Clayton says, is a profession of shock and dismay from the owner of the hosting service when the journalist calls about the jihadi website on his server.

"And he pulls the plug, which annoys the FBI—which has been tapping it—no end."

Cite this article: