PER CONCORDIAM ILLUSTRATION

BASE OF OPERATIONS: THE INTERNET

Europe devises new strategies to confront violent extremists who lurk online

By *per Concordiam* Staff

The Internet is one of the extremist's most valuable tools. Chat rooms, message boards, e-magazines, videos and social media are used by radicals to recruit and train new members, plan and coordinate attacks with cohorts across the world and raise money through donations and online fraud. The growth of radical material online poses a serious threat to the world, and the European Union and its partners are working together to find solutions. "This is a very serious issue," then-United Kingdom Security and Counterterrorism Minister Pauline Neville-Jones warned at a 2011 counterradicalization symposium. "The Internet plays an ever more significant role in the sedulous promotion of terrorism."

Just as the Internet is becoming tightly interwoven in our everyday lives, it is also assuming a larger role in criminal and extremist activities. The number of terrorist websites has soared during the past decade, and so has the volume of material they post online. In the time that it takes counterterror groups to discover and eradicate terrorist propaganda, the videos, photos and violent exhortations have already been anonymously copied and posted to other sites. In the UK, the Internet plays a role in nearly every national security investigation conducted by police and intelligence agencies, the United States think tank Rand Corp. said in a report published in November 2013. The U.S. government says it monitors about 5,000 jihadi websites and closely watches about a hundred it believes are most hostile.

INTELLIGENCE COLLECTION

Merely removing malicious online material is not a silver bullet to end Internet radicalization. Counterterror experts derive valuable information from online activity and admit there are benefits to leaving the material up. "The inclination may be to shut down radical websites, filter contact, and control what the public can access; however, that approach is not only ineffective, but also counterproductive," said Dr. Peter Neumann of the Bipartisan Policy Center in Washington, D.C.

Experts suggest that extremist online activity and propaganda provide intelligence such as who is talking to whom and what ideas they are discussing — all significant pieces of a puzzle that could lead to early intervention and prevent violence. German officials were able to issue early warnings about the Madrid train bombings in 2004 because they were monitoring online chat rooms, according to an April 2011 Council of Foreign Relations article.

Al-Qaida leader Anwar al-Awlaki, one of the biggest threats to U.S. homeland security before he was killed in 2011, routinely used emails, blogs, chat rooms, and al-Qaida's online magazine Inspire to entice disgruntled Americans to attack their own country. Al-Awlaki and Maj. Nidal Hasan, a U.S. Army psychiatrist who killed 13 people in a shooting rampage on Fort Hood military base in 2009, exchanged lengthy emails.

Online extremists have grown inventive. They have found ways to communicate via email without actually sending the email. They use a single account, compose an email message and leave it in the drafts folder. The intended recipient can log into the same account and read the unsent

message to avoid detection. Conversely, officials have fashioned phony websites and posted fictitious information to trap extremists and taint the reliability of information that violent radicals receive online. Osama bin Laden refused to use the Internet out of fear that his identity and location could be revealed.

SOCIAL MEDIA

Message boards and comment forums, once the extremist's go-to means of communication, have lost popularity in favor of social media. Al-Qaida opened its official Twitter account in September 2013, according to *The Washington Times*. The members-only site attracted 1,532 "followers" on its first day. U.S. counterterror officials said some of the followers were high-profile digital jihadists. "We've seen terrorist groups make increasingly effective use of social media, particularly Twitter and Facebook," counterterror expert Patrick Poole said in the same article. Officials expect social media to be a "major intelligence target for foreign governments tracking al Qaida through its online devotees."

> "We've seen terrorist groups make increasingly effective use of social media, particularly Twitter and Facebook."
>
> — *Patrick Poole*

In the past, forum administrators were often quick to remove offensive and inflammatory messages, hindering communication among extremists. However, social media sites have been more lenient about what material is posted. Recently, the posting of a decapitation video prompted Facebook to issue more restrictive rules. After some back and forth, the site decided to prohibit any video that "improperly and irresponsibly glorifies violence."

RADICALIZATION FAST TRACK

Because the Internet never closes, it can accelerate the path to radicalization. Chat rooms, social media sites, message boards and video-posting sites allow like-minded individuals to exchange information 24 hours a day. Al-Qaida fighters use chat rooms, and the Web provides a plethora of information on past terror plots and countless "how-to" videos and articles on homemade explosives. "It offers a 'one stop shop' for all the information that an extremist may seek out, or by which they may be influenced," Rand cautions. Moreover, the Internet broadens the range of people extremists can reach. It can break down barriers such as ethnicity, gender and country of residence.

SOLUTIONS

The most effective way to counter terrorists' use of the Internet is to counter their messages and collect intelligence on the information they post, the London-based Institute for Strategic Dialogue (ISD) concluded in a 2011 report. The development of countermessaging can take three forms: dissecting the ideology, undermining credibility and mocking the extremist, and promoting a positive alternative. The ISD suggests that countering the message is most effective, but also challenging.

Religious edicts that counter jihadist narratives and point out inconsistencies between religion and violence are successful. The messenger can make all the difference. Former extremists hold much more credibility delivering the countermessage. Another method is to attack their effectiveness, explaining that terrorists are harming the very communities they claim they are protecting. When victims of terrorism come forward and tell their stories, they undermine the extremist agenda.

The public and private sector working cooperatively to defend against the malicious use of the Internet can serve as a powerful counterterror tool. Because the Web is largely operated by the private sector and intelligence services by governments, information sharing between the two is crucial.

Twelve European countries, the United Nations Office on Drugs and Crime, and numerous think tanks and law enforcement agencies sought to create a program to do just that. Clean IT, a

two-year project that ended in March 2013, issued a final report that recommended seven proactive and 12 reactive best practices. They include prominently displaying strict website terms and conditions prohibiting terrorist activities; expanding programs to warn children, teenagers and young adults of the dangers of terrorist groups online; and establishing flagging mechanisms to alert officials that terrorists are using their online service. Google, parent company of YouTube, has incorporated a flagging mechanism that provides users with a "flag" button located below every video to alert moderators around the clock of videos that violate guidelines.

Although the EU's stance is that the bulk of counterradicalization should take place at the local and national level, it has implemented strategies to assist in this effort. The European Council's "Check the Web" initiative focuses on cooperation among EU countries to share the task of monitoring open Internet sources. The Home Affairs office of the EU started the Radicalization Awareness Network (RAN), which aims to facilitate information sharing among people who work directly with at-risk individuals within the EU. RAN focused its May 2013 meeting on the role of the Internet in radicalization.

The UK's Prevent strategy, part of its larger counterterrorism effort known as CONTEST, focuses on community awareness and relies on the public to report when it sees someone access violent extremist material online in places such as coffee shops and Internet cafes.

AWARENESS AND EDUCATION

Counterextremism education for parents, teachers and the general public to recognize warning signs in youth are essential for prevention. "We know that in the UK, groups gather to view the preaching of violent men located many thousands of miles away and that this does have a powerful effect in young minds," Neville-Jones said.

GETTY IMAGES

The first edition of the Yemen-based al-Qaida in the Arabian Peninsula's online magazine Inspire includes an article called "Make a Bomb in the Kitchen of Your Mom."

Employing effective deterrence strategies, working together to share information, implementing counternarratives and educating youth and communities are important steps to prevention. The UK government alone has removed 5,700 "items of terrorist material" from online in the past couple of years.

"But it is clear we need to do more," UK Prime Minister David Cameron said in a June 2013 *Telegraph* article. "It is not simply enough to target and go after violent extremists after they've become violent. We have to drain the swamp in which they inhabit. It means going through all of these elements of the conveyor belt to radicalization and making sure we deal with them." □