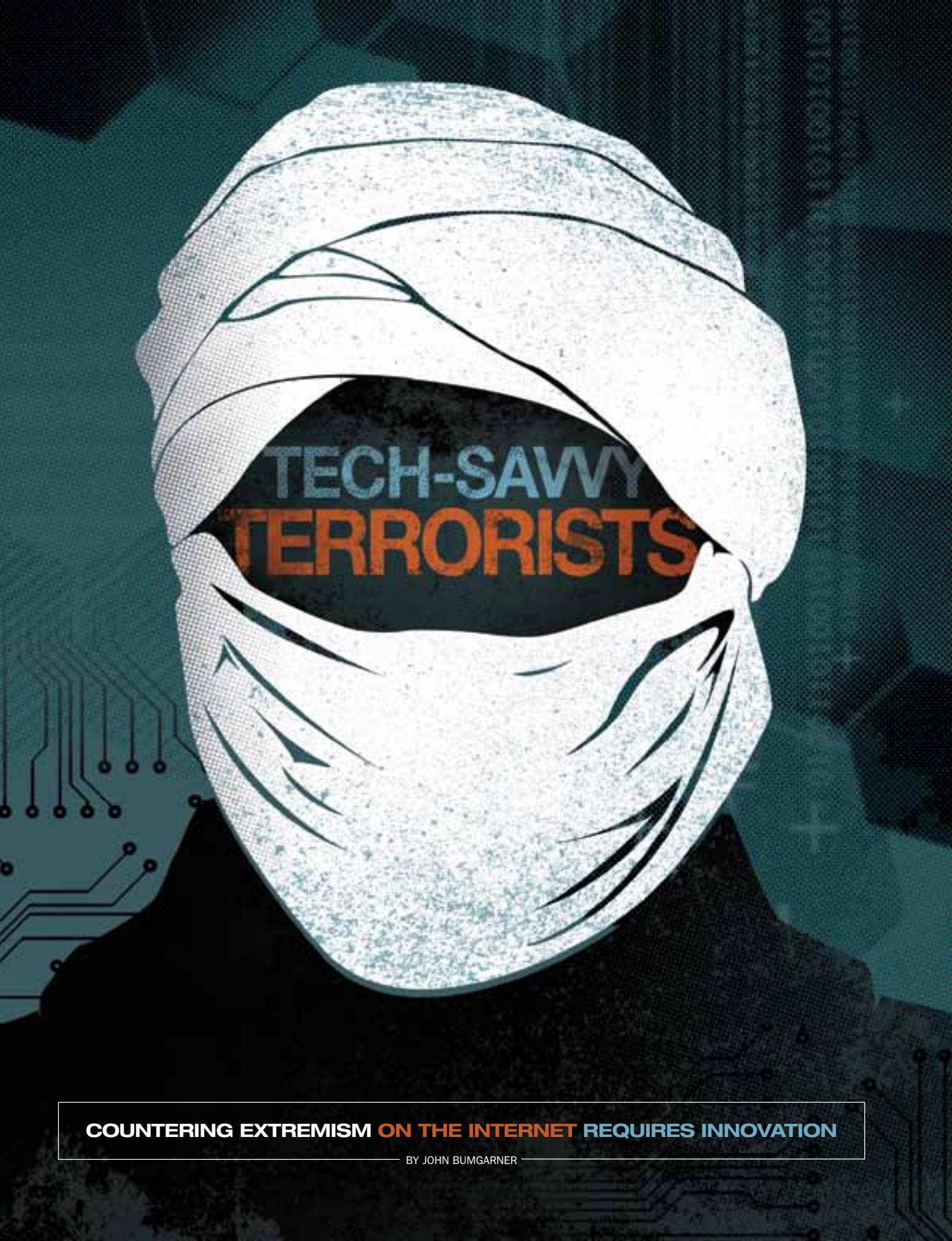

COUNTERING EXTREMISM ON THE INTERNET REQUIRES INNOVATION

BY JOHN BUMGARNER

On a bustling evening in late November 2008, automatic gunfire ripped apart Mumbai. When the shooting stopped, 175 people were killed and 308 were wounded. Terrorist attacks on Indian soil are nothing new, but this horrific event conducted by members of the Lashkar-e-Tayyiba (Army of the Righteous) had an important component that previous terrorist incidents lacked:

the use of 21st-century technology.

In the tragedy's aftermath, authorities discovered that the Mumbai terrorists had employed technology in all phases of their operation. During the planning phase, the attackers conducted virtual reconnaissance of their targets using Google Earth. The high-resolution images provided by Google allowed the terrorists to plot their suicide mission with great precision, even down to the entrances and exits to be used at the primary target locations. Google also provided the attackers with the geographic coordinates for their targets, which were programmed into GPS devices. Using this information, the attackers were able to navigate to their sea infiltration point undetected and under cover of darkness. The utilization of technology greatly reduced the likelihood the attackers would encounter unforeseen obstacles along their assault paths, increasing the effectiveness of the attacks.

During the execution phase of the Mumbai assaults, the terrorists used cell phones configured with Subscriber Identity Module cards obtained from different countries. The attackers used these phones to provide status updates to their handlers, who were using Voice over Internet Protocol, or VoIP, channels to mask their physical locations. Investigators speculated that the handlers used real-time television coverage to track the location of the police units and counter-terrorism commandos that had responded to the attacks. The handlers reportedly updated their operatives on these police locations using the Short Message Service, or SMS, available on their cell phones. These communication steps made it more difficult for law enforcement agencies to intercept the calls or trace them after the attacks occurred.

Indian authorities have voiced concerns that future terrorist attacks in their country could be coordinated using either BlackBerry cell phones or the popular VoIP service Skype. One of the unique selling points of both these communication channels is strong encryption capabilities. The Indian government recently demanded that the manufacturer of the BlackBerry device, Canadian-based Research In Motion, provide the government with the keys to unscramble the SMS and e-mail messages being transmitted. Indonesia has also demanded that the company provide encryption keys to government authorities or face legal consequences.

Evidence shows that terrorist organizations have not only used commercially available encryption

programs but have developed their own sophisticated applications as well. For example, in response to growing fears about eavesdropping, the Global Islamic Media Front released an encryption application called Asrar Al-Mujahidin ("Mujahedeen Secrets") first on several restricted Web forums and later on dozens of publicly accessible file-sharing sites. Mujahedeen Secrets supports several advanced encryption algorithms, including the Advanced Encryption Standard, or AES. In 2001, the U.S. government approved the AES to safeguard sensitive public information, and in 2003, the National Security Agency approved the AES to protect top-secret information. The terrorist organization Hezbollah has praised the brilliance of encryption programs such as Mujahedeen Secrets, which allows its members to communicate without fear that their messages will be deciphered by the Americans.

THE ASSOCIATED PRESS

An Indian Soldier calls additional forces forward as the Taj Mahal hotel burns in Mumbai after terrorists attacked in November 2008. The attackers used the Internet to plan the assault, which left hundreds dead and wounded.

TERRORIST CLASSROOMS ON THE NET

Extremist groups have also distributed training materials on both public and restricted Web portals. These materials include copies of training manuals used by the U.S. military, especially the U.S. Army, which are available on many extremist sites. The manuals describing combat techniques further link these extremist groups to violence. For example, the TM 31-210 Improvised Munitions Handbook, created by the U.S. Army for the Special Forces, has been distributed on the websites of extremist groups. This technical manual offers practical advice on the construction of improvised explosive devices, or IEDs, from materials that may be readily purchased from most home improvement centers. Although the techniques described in this manual have been successfully exploited by terrorist groups for decades, the Internet has clearly lowered the cost of distributing these instructions. Other available manuals distributed on websites frequented by extremists have included The Terrorist's Handbook, The Anarchist Cookbook and the Mujahedeen Poisons Handbook.

Many terrorist or extremist organizations have also developed and distributed their own training materials via the Internet. Improvements in streaming online video have expanded the capabilities of these virtual training aids. Web-based distribution confers other advantages to the groups as well. For example, Web-based training may be more secure than physical training camps, which are vulnerable to physical attacks. Furthermore, aerial bombardment or skirmishes with ground forces pose a threat not just to the training camps but also to the people who attend them. By contrast, if a Web-based training site is shut down, its members remain unharmed and live to fight another day.

Web-based distribution also allows terrorist organizations to train more individuals in combat techniques more efficiently. Web-based training materials may be disseminated quickly to members of extremist groups throughout the world. The materials may be downloaded (duplicated) by members at almost no additional cost and may be used by a large number of members simultaneously. These materials may also aid extremist organizations in their efforts to recruit and indoctrinate new members.

Virtual training materials developed by terrorist groups cover a wide range of topics, including IED construction and guidelines on the use of shoulder-fired, surface-to-air missiles. Another terrorist video demonstrates techniques for making a vehicle-borne improvised explosive device, or car bomb. Car bombs have been used successfully in many terrorist attacks in the Asia-Pacific region, including Bali, Indonesia, in 2002; Islamabad, Pakistan, in 2008; and Narathiwat, Thailand, in 2009. Currently the majority of terrorist bombs are delivered by suicide bombers, but GPS technology provides another method. This technology allows a terrorist organization to develop a bomb with a GPS-enabled detonator coupled with a timing device that can be delivered in multiple ways to a target location.

Many videos advertise the effectiveness of radical violence by extremist groups. For example, some videos show the tactical effectiveness of roadside bombs against coalition forces in Iraq. Others document brutality inflicted by extremist groups on their captives. Some videos highlight the path to martyrdom chosen by other group members. The As Sahab Foundation for Islamic Media Publication, which has supported various organizations known to be Al-Qaida associated movements, or AQAM, created a unique video depicting the 2008 bombing of the Danish embassy in Pakistan that blends several of these elements. The video begins with an interview with a suicide bomber. It then uses computer animation to simulate a suicide bombing attack on the Danish embassy, which ends in a massive fireball. The video has been widely distributed on many websites, including YouTube.

THE TERROR SOCIAL NETWORK

Extremist groups are also commonly using many of the most popular social networking sites, including Facebook, Friendster, LiveJournal and MySpace, to communicate with sympathizers and spread propaganda to the masses. For example, the Moro Islamic Liberation Front in the Philippines maintains a Facebook page, and several purported members of Abu Sayyaf maintain MySpace accounts. By providing access to a large network of users, these portals facilitate worldwide recruiting and fundraising by these groups.

The microblogging service Twitter can be used by terrorists to distribute operational information to members anywhere in the world. For example, the following encrypted text contains the geographic coordinates for a popular Asian tourist site, the attack method that will be employed, the date to launch the attack and the next Twitter account that will be used to disseminate operational information:

The architecture for private, quasi-anonymous communication that is provided by many social networking sites shelters members of extremist organizations from detection by most law enforcement agencies. Some social networking sites feature user controls that allow extremist groups to prevent or detect infiltration. For instance, individuals who seek to become group members might have to be approved or invited to join the group. Individuals requesting membership may thus be thoroughly vetted before they are permitted to view the content on the group's website or to participate in forum discussions with other group members. Additionally, many social networking sites permit groups to monitor forum content or other website activities. These elements are critical to ensuring the group's operational security.

A Rapid Action Force policeman patrols outside the Taj Mahal hotel in Mumbai after terrorists attacked in November 2008. The attackers used Internet tools to plan the assault.

EASY DISTRIBUTION

Terrorist organizations have distributed other applications and programs on the Internet as well. Cyberspace has many digital repositories maintained by extremists that offer bootleg copies of commercially available programs that might help members evade electronic detection. For example, some applications anonymize Internet surfing activities. Others are designed to perform advanced anti-forensic tasks, such as securely deleting files via methods approved by the U.S. Department of Defense or erasing incriminating Internet surfing trails from a member's computer.

Video applications also play a pivotal role in the psychological warfare operations of extremist groups. Many videos direct persuasive communications toward a specific audience, for example, educated but disenfranchised individuals

THE ASSOCIATED PRESS

GEOEYE

Terrorists used satellite images online to plot their attack on Mumbai's Taj Mahal hotel, seen here to the left of the center, on the water.

to propagate the groups' ideologies. Widespread campaigns of propaganda and possibly disinformation allow a terrorist organization to leverage the involvement of third parties who are sympathetic to, if not directly involved in, the organization's cause. AQAM organizations are increasingly featuring members who speak English in videos aimed at Western audiences. The release of a video may also be timed to achieve the greatest possible impact. For example, a cell-phone video of an IED attack may be released immediately following the event, which attracts media attention and possibly an ancillary following by the general public. The video may thus intensify the emotional response of the public to an attack that has taken place. Several terrorist groups have used YouTube to distribute motivational videos about their armed struggles. For example, the Liberation Tigers of Tamil Eelam, or LTTE, of Sri Lanka has a training video of its forces posted on that website.

a. An Indian woman checks out damage to the Taj Mahal hotel, which was attacked by terrorists in November 2008.

b. To combat extremists from 10 high-risk countries, Australian border officials plan to use electronic fingerprints and face scans.

c. People use computers at in Internet café in Shanghai in January 2010. Extremists launched sophisticated attacks against human rights activists around the world using Google's Gmail service.

EMERGING ATTACK CAPABILITIES

Most terrorist organizations operating in the Asia-Pacific region have mastered launching kinetic attacks but are still in the infant stages of understanding how cyber attacks can be employed effectively against digital targets. Some of the best computer programmers in the world live within the region and fully understand how to develop cyber threats. In 2000, one of the most disruptive computer worms in the history of the Internet, known as the "Love Bug," was developed by programmers living in the Philippines.

One of the most basic cyber attack techniques available to terrorist groups is distributed denial-of-service. Militants can launch these disruptive attacks by renting computer systems from cyber criminals who specialize in providing this service. An underutilized technique for launching these attacks is the distribution of software applications to sympathizers through social networking portals or restricted Web forums. Such applications could be designed to launch a large-scale cyber attack against any digital target in the world. Islamic terrorist groups have called for followers to conduct "www Jihad" against infidels. Several terrorist groups are already developing the necessary skills to forge an effective cyber assault against various government digital targets in the future. Terrorist organizations have realized that the Internet is not a target but a weapon that can be wielded with great precision.

By providing a number of applications and services that substitute for face-to-face contact and physical training camps, the Internet helps extremist organizations promote their agenda. Ethnonationalist or religious militant groups can easily use the Internet to recruit, indoctrinate and train members to wage violent attacks within any nation in the Asia-Pacific region. As the Mumbai attacks showed, violent extremists can use the Internet to plan and coordinate physical acts of terrorism. Furthermore, some radical extremist groups have begun to investigate ways to use the Internet itself as a weapon to launch cyber attacks that would have catastrophic consequences in the real world. Extremist groups will use the Internet more and more as their members gain additional technical knowledge and as technology becomes ubiquitous in the world.

As cyber extremist elements within the Asia-Pacific region continue to flourish, efforts to combat them must also grow larger and more sophisticated. In an open, democratic society, countermeasures must strike a difficult balance, thwarting terrorism without constraining liberty. □

* John Bumgarner is chief technology officer for the U.S. Cyber Consequences Unit. He served as an expert source for *Business Week*, CNN, Jane's Defense, *The Wall Street Journal* and *The Guardian* in London.

14 WAYS TO COUNTER INTERNET EXTREMISM

COMPILED BY TIMOTHY L. THOMAS, ANALYST AT THE FOREIGN MILITARY STUDIES OFFICE AT FORT LEAVENWORTH, KANSAS.

01 Mute extremist messages.

02 Turn extremist groups' weaknesses against them.

03 Emphasize extremist organizations' mistakes.

04 Plant fake e-mail messages and website posting to seed confusion, dissent and distrust among extremist organizations.

05 Amplify speeches and writings of prominent clerics who renounce terrorist violence.

06 Identify territory that terrorists cherish, and damage that territory. For example, emotional territory such as a terrorist's reputation.

07 Identify, manipulate and even destroy terrorist territory on the Web.

08 Use captured computer hard drives to learn how to develop counter messages.

09 Release seized videotapes to show terrorist brainwashing session with children including hate cartoons and extremists' "camps" for children.

10 Release letters that demonstrate poor morale within extremist organizations.

11 Determine what dishonors extremist organization and undermines their rhetoric on the Web.

12 Undercut extremists' popular or theological legitimacy for actions such as their moral legitimacy for employing weapons of mass destruction.

13 Persuade extremist "support networks" to stop helping extremists and hold them accountable.

14 Develop technical systems that identify the source of unconventional weapons and components.

Thomas, T. "Countering Internet Extremism," IO Sphere Winter 2009.