

'Western intelligence agencies need central capabilities to monitor the terrorist web'

ISSUES &

FIGHTING THE VIRTUAL WAR

FIRST OF FOUR PARTS



MIKE FAILLE / NATIONAL POST

Terrorists and rogue states are moving their battle to the Internet. In a four-part series, our authors explain how to fight this evolving menace

'THE CODE IS MIGHTIER THAN THE SWORD'

MARK DUBOWITZ
AND LARRY FOOTER

The Long War against radical Islam is a war of ideas as much as a war of arms. Yet, for too long, the incitement and violent propaganda from Internet platforms operated by violent Islamist extremists have gone unnoticed and unanswered.

Today, such neglect is not an option. As we have been warned by Harry Wingo — a former Navy SEAL who now serves as Google's Washington, D.C. policy counsel — "the code is mightier than the sword."

Internet code may have created enormous wealth for Mr. Wingo's bosses. But it is also an operational weapon in the hands of terrorist groups to indoctrinate, recruit, train, and finance the next generation of terrorists. Increasingly besieged on the battlefield, al-Qaeda, Hezbollah, Hamas and their Islamist brethren now seek anonymity and freedom of movement online through a vast and sophisticated terrorist web network. To counter their influence, policymakers and counterterrorism officials need to treat these outlets as indistinguishable from the terrorist organizations that use them.

The threat is real. A declassified April 2006 U.S. National Intelligence Estimate concluded: "The radicalization process is occurring more quickly, more widely, and more anonymously in the Internet age, raising the likelihood of surprise attacks by unknown groups whose members and supporters may be difficult to pinpoint. We judge that groups of all stripes will increasingly use the Internet to communicate, propagandize, recruit, train and obtain logistical and financial support."

Through as-Sahab, its dedicated media wing, the bin Laden network has built a formidable infrastructure to export its violent ideology. In its definitive report on as-Sahab, the U.S. Senate Committee on Homeland Security and Governmental Affairs equated al-Qaeda's media presence with that of many Western corporations in terms of sophistication. According to the Senate Committee report, as-Sahab has attracted Western attention in part because its videos have included original sermons from senior al-Qaeda officers, such as Osama bin Laden and Ayman al-Zawahiri. In 2007, as-Sahab is known

to have produced 97 original videos, a six-fold increase from 2005.

As-Sahab leverages its products through Internet "clearinghouses," which act as middlemen in distributing terrorist media to "mirror sites," whereupon the videos go viral on jihadist web forums and on popular Western sites such as Archive.org and YouTube.

All this is part of a deliberate strategic goal outlined by al-Qaeda's senior leadership. In a letter to former Iraqi al-Qaeda leader Abu Musab al-Zarqawi, Ayman al-Zawahiri, al-Qaeda's second in command, wrote: "We are in a battle, and more than half of this battle is taking place in the battlefield of the media ... we are in a media battle in a race for the hearts and minds of our people."

Major General John M. Custer III, Commanding General of the U.S. Army Intelligence Center, underscores the impact of online terrorist media: "I see 16, 17-year-olds who have been indoctrinated on the Internet turn up on the battlefield ... You start off with a site that looks like current news in Iraq. With a single click, you're at an active jihad attack site ... You can see humvees blown up ... small arms attacks ... Next link will take you to a motivational site, where mortar operatives, suicide bombers, are pictured in heaven [providing] religious justification for mass murder."

Terrorist online platforms are a critical part of the battlefield on which the Long War against violent Islamist extremism is being fought. If they hope to persevere, Western democracies need to take aggressive and direct action against these media properties.

What can be done? A great deal as it turns out — from shutting down these sites to exploiting them for counterterrorism purposes. To understand how, think of the terrorist web as two different platforms: (1) interactive forums, discussion groups, blogs and chat rooms used by jihadists to communicate and direct with each other and attract and plan new recruits; and (2) static web pages of violent propaganda. While the former can provide Western intelligence agencies with vital information about potential attacks, the latter frequently contain little if any probative value beyond their violent messaging.

The goal should be to shut down those sites that yield little in the way of actionable intelligence while infiltrating, monitoring and countering

the more dynamic sites that serve as operational tools for the terrorists. An effective online strategy should serve to limit and discredit the jihadist message, deny safe haven to terrorists on the Internet, thwart their ability to obtain support from a vulnerable online population, and continue to monitor their communications on web forums.

A first step: The U.S. and Canada should designate or criminalize terrorist sites as terrorist entities.

The U.S. Treasury Department has already designated Hezbollah's *al-Manar* and the Iraqi-Syrian *al-Zawraa* television channels for their role in providing operational support in furtherance of terrorist attacks.

'You start off with a site that looks like current news in Iraq. With a single click, you're at an active jihad attack site'

These designations should be expanded to include websites, terrorist video production units, media companies, and website operators. Governments need to freeze their assets, and make the provision of material support to these entities and individuals a criminal offense.

The private sector must also be encouraged to monitor and self-regulate. Policymakers should encourage media entrepreneurs to follow the lead of Google, which, in 2008, after requests from Senator Joseph Lieberman and other members of Congress, removed numerous violent al-Qaeda videos from its YouTube video sharing service. In making the decision not to facilitate the transmission of terrorist media, Google made a sound business choice to avoid the real reputational risk of

being identified, fairly or not, with the activities of a terrorist organization.

For those companies not willing to self-regulate, regulations should be adopted for "Terms of Service" agreements between Internet companies and their clients, focused on preventing the incitement of violence. Internet providers that repeatedly aid terrorist entities by hosting their websites should be fined to the full extent of the law.

Western counterterrorism and intelligence agencies also need centralized capabilities to monitor and respond to the terrorist web. Co-ordinated strategic information campaigns should be waged against these groups, including cataloging, tracking and continuously updating a database of terrorist websites, website operators and chat room participants.

Discrediting the jihadist cause also is a critical aspect to winning the hearts and minds of the primarily young online audience. Information campaigns must be conducted against Islamist terrorists by widely publicizing their atrocities on the Internet. Too few Muslims, for example, know about incidents such as the February 2008 terrorist attack in which, according to Britain's *Daily Mail*, al-Qaeda rigged two unsuspecting women who were afflicted by Down's syndrome with remote-controlled bombs and detonated them in a Baghdad market killing 99 people.

Sophisticated technology has an important role to play in countering the terrorist web. While some portions of the terrorist web are out in the open, other parts operate in an area of the Internet commonly referred to as "the Deep Web." Akin to an ocean, the Internet has surface pages, but a significant portion lies beneath that surface, out of reach of most popular search engines.

A handful of companies have developed data intelligence technologies that give access to sites traditional search engines cannot find. The U.S. intelligence community and military use these technologies to transform web data from terrorist sites into actionable intelligence.

For example, certain applications can crawl millions of domains simultaneously, a task impossible for human analysts alone. Since this volume of data, including dynamic content from the most complex websites, can be overwhelming for intelligence analysts, applications automatically

extract and analyze only the data of higher intelligence value. They also use "anonymizer" tools to hide the computer user's identity to try and keep the intelligence analyst from being shut out by terrorist web masters.

As a last resort, terrorist media's infrastructure and personnel represent viable military targets. The precedent exists: During the war in Kosovo, NATO planes bombed the Belgrade-based headquarters of Radio Television of Serbia — an attack that was justified by the Alliance as a legitimate way to end the broadcasting of Slobodan Milosevic's violent call to arms. Today, recognizing the dangers of terrorist radio, U.S. officials are jamming the FM radio signals of Pakistani terrorist groups to prevent them from assisting in the planning and execution of attacks. In the future, more direct action may be necessary.

The terrorist groups — and their Western apologists — can no longer pretend that these terrorist media sites are legitimate outlets deserving of free-speech protection. In fact, violent incitement has been prosecuted as a war crime, initially at the Nuremberg trials against the Nazi regime after World War II and, in 2003, against three Rwandan media executives who used Rwanda's Radio Mille Collines to call for the extermination of Rwanda's Tutsis. At that time, Reed Brody, legal counsel to Human Rights Watch, in supporting the Rwanda decision, concluded that, "If you fan the flames, you'll have to face the consequences."

By doing just that — by inciting attacks, by actively recruiting and fundraising and providing pre-attack intelligence and operational assistance for terror attacks — today's terrorist Internet sites are doing more than fanning the flames. They are providing the match, the gasoline, and the arsonist. It is high time that we treated terrorist code as being as dangerous as the sword.

National Post

■ "Fighting the Virtual War" is presented in collaboration with the Foundation for Defense of Democracies (FDD), a Washington, D.C.-based policy institute focused on terrorism. Mark Dubowitz is executive director of the FDD. He previously worked in software management and technology venture capital. Larry Footer is FDD's chief technologist. He is also the CEO of a New York-based software company.

TOMORROW

MILT MALTZ

Turning power lines into battle lines