Combating Terrorism on the Free Highway

raphael cohen-almagor, University of Hull
Raphael Cohen-Almagor

Cooperation is vital in combating the abuse of the Internet by terrorist groups.

The Internet has enabled transnational jihad based on a decentralized network that overcomes the limitations of face-to-face interaction. Terrorists are making the most of the Internet to: 1) find essential information, 2) communicate, and 3) coordinate among each other in order to wage violent anti-social operations.

Finding Essential Information

Jihadi websites have several sections. The most important is usually the religious section, which features Quranic references to jihad, the different ways jihad can be expressed, aspects of martyrdom, fatwa (opinions on matters pertaining to Islamic law) explaining who can be targeted legitimately, and online doctrinal consultations with religious leaders. In the jihad section, would-be recruits are encouraged to join the battle. Some general advice is given, such as the best routes into warzones as well as the names and locations of sympathetic mosques. Galleries of martyr portraits are accompanied by their last testaments, often in a video clip. Many sites also have an IT section where contributors are urged to share their knowledge and develop new ways of using cyberspace to further jihad. Furthermore, some jihadi sites have a women’s section where wives and mothers are urged to support their men in jihad and help them in the psychological battle against what one site described as “that disease, the weakness which loves life and hates death.”

There is also an immense amount of “how-to” material together with the staple violent propaganda. Multiple password-protected forums contain extensive literature on explosives. There are tutorials on viruses, hacking stratagems, the use of secret codes, encryption methods, Tor and other anonymity tools. Bomb-making knowledge is available on jihadi websites in the form of very detailed step-by-step video instructions showing how to build improvised explosive devices (IEDs). There is strong evidence that such online instructions played a critical role in the March 2004 Madrid bombings, the April 2005 Khan el-Khalili bombings in Cairo, the July 2006 failed attempt to bomb trains in Germany, and the June 2007 plot to bomb London’s West End and Glasgow.

Communicating

Networking

Jihadi websites allow isolated young Muslims to engage with a worldwide network of like-minded people striving against what they perceive as a common enemy and with a singular unity of purpose. They offer these individuals a space to develop friendships and support, and prove the existence of the ummah, or imagined Muslim nation. In this way, the Internet bridges the gap between isolated potential jihadists and those already active within transnational jihad circles. Connections may develop on popular social networking sites such as Facebook and Twitter and then continue on more specific jihadi forums and websites.

Propaganda and Indoctrination

Most radical and terrorist organizations use the Internet as a vehicle for ideological indoctrination. Al Qaeda has been particularly successful in its use of multimedia propaganda, producing pre-recorded video and audio, photographs, and written documents. Islamist zealots are also developing computer games and promoting hip-hop artists in order to spread radical ideology to reach individuals within traditionally adversarial populations. Nearly every insurgency operation in Iraq was filmed and posted on a number of sites and bulletin boards accompanied by jihadi songs. The bloodshed was presented as heroic and glorious, and the accompanying text promoted jihad. The attempt to target traditionally adversarial populations is also seen in the publication of an English language jihadist magazine called Inspire by Al Qaeda in the
Arabian Peninsula (AQAP). Known for its high production standards, the magazine targets English-speaking Muslims, encouraging them to engage in militant activity where they live.

**Recruitment**

There are numerous cases of average, even non-religious citizens becoming radicalized by jihadist websites, leaving them vulnerable to terrorist recruitment. The content of such websites usually consists of enemy demonization, justification of violence, and a general background of the jihadi group, its platform and objectives. The websites try to be effective as they compete with each other on the attention of potential followers. Interactive technology is used to connect with those who seem receptive to the jihadi messages and ideology.

**Coordinating**

Information technology has enabled terrorist organizations to receive and share knowledge globally. The Internet has proven to be an excellent vehicle by which information about travel, training, targets, tactics and a host of other useful organizational details is displayed. Instructions, maps, diagrams, photographs, tactical and technical details are often sent over the Internet in encrypted formats, using onion routers such as Tor that hide the Internet Protocol (IP) address.

Al Qaeda members used the Internet extensively in planning and coordinating the attacks of 11 September 2001. Mary E. Galligan, who supervised the FBI’s investigation of the attacks, said that the Internet was a vital channel for coordination. Galligan asserted that Al Qaeda terrorists learned the methods used by the US to combat terrorism and studied soft spots and targets. They refrained from using cell phones, as they knew cell phones could be traced. Instead, they used the Internet, prepaid phone cards, and face-to-face meetings in Spain. Email was used to transmit messages between the terrorists. They looked for American flight schools on the Internet while they were in Germany, and used public library terminals for communications and data. At many public libraries, people can simply walk up to a terminal and access the Internet without presenting any form of identification. Within two weeks of the 9/11 attacks, the US had located hundreds of e-mails linked to the hijackers, in English and Arabic, sent before 11 September, some of which included operational details of the planned terrorist assault.

**Fundraising**

Crucial to the coordination of terrorist attacks is the provision of necessary funds. The Internet has been a crucial enabler in this regard too, with terrorist groups raising funds via some or all of the following five main methods:

1) **Appeals via e-mail or directly through websites**
Hamas has in the past circulated appeal letters to various newsgroups. Hezbollah supplied bank account information to those who solicit the group by e-mail and posted its bank account information directly on several of its websites.

2) **Selling goods**
Many sites offer online “gift shops,” where visitors can purchase or download free posters, books, videos, pictures, audiocassettes and discs, stickers, badges, symbols, and calendars.

3) **Side businesses that are not identified as group-owned but are nevertheless associated**
There are links between terrorism and organized crime, especially in spheres concerning illegal migration, corruption, economic crime, illicit drugs, arms trafficking and money laundering. Hezbollah has coordinated the transportation, distribution, and sale of multi-ton bulk shipments of cocaine from South America. Large amounts of cash were smuggled to Lebanon, and several Lebanese exchange houses utilized accounts at the Beirut-based Lebanese Canadian Bank (LCB). The proceeds were laundered through various methods which included the sale of used cars in the United States to African nations, mixing legitimate business with drug money which eventually found its way to Hezbollah.

4) **Online organizations that resemble humanitarian charity groups**
Some charity organizations in the USA were in the service of Hamas and the Hezbollah until they were closed down. Charities acted as legitimate front organizations which raised money from across the globe
5) Fraud, gambling, or online brokering
According to the United Kingdom’s Financial Services Authority (FSA), terrorist groups launder their money through online firms. Online brokerage and spread-betting firms are particularly vulnerable to exploitation by terrorist groups because they are under-regulated and do not perform thorough checks on their investors. Younes Tsouli, Waseem Mughal and Tariq Al-Daour, based in London, working for Al Qaeda in Iraq, stole money through online gambling sites. With different Trojan viruses, the three terrorists managed to raise more than US$3.5 million to buy web hosting services in order to show more influential videos of al-Qaeda.

Combating Terrorist Activities Online

Combating terrorist activities online demands resources and capabilities that most of us – normal citizens – do not have. The prime responsibility lies with ISPs (Internet Service Providers), governments, and the international community at large. As terrorism is a global phenomenon, it is necessary to fight against it globally via diligent cross-country cooperation.

ISP Responsibility
Like any other industry, there is a need to assure a certain security level on the Internet. Many ISPs hosted terrorist sites and helped the cause of transnational jihad. Some did it knowingly while others did it inadvertently. InfoCom Corporation in Texas, for instance, hosted websites for numerous clients in the Middle East. Founded by Mousa Abu Marzook, a senior official in Hamas, it served more than 500 Saudi Internet sites and notable Palestinian Hamas organizations, including the Islamic Association for Palestine and the Holy Land Foundation for Relief and Development. InfoCom also served to launder money from Saudi Arabia and the Gulf states to sponsor Hamas activities. While the InfoCom Corporation knowingly participated in terrorist activities, Fortress ITX unwittingly hosted a jihadi website that urged attacks against American and Israeli targets. This website was shut down when Fortress learned about the content from a reporter. To avoid playing into the hands of terrorists requires oversight and proactive steps. ISPs are, however, reluctant to monitor their servers for economic reasons.

International Cooperation
Halting the flow of funds via the Internet to terrorist organizations is a difficult and time-consuming task. Sites and accounts are closed and re-opened under different names very swiftly. As many terrorist organizations have set up charities in the real as well the virtual worlds, multilateral bodies such as the Financial Action Task Force (FATF), which was established to combat money laundering and terrorist financing, are instrumental in sharing information about the global charitable sector, improving oversight of national and international charities, devising methodologies for detecting terrorists masquerading as charities, and establishing international standards to combat such abuse.

On 8 September 2006, the United Nations adopted a Global Counterterrorism Strategy. The strategy, in the form of a resolution and an annexed Plan of Action (A/RES/60/288), is a global instrument designed to enhance national, regional and international efforts to counter terrorism. It marked the first time that all Member States had agreed on a common strategic approach to combat terrorism and resolved to take practical steps to fight it. These practical steps ranged from strengthening state capacity to better coordinating UN counterterrorism activities.

The European Union police agency, Europol, built an information portal to allow for the exchange of information on militant website monitoring. The portal includes a list of monitored websites as well as statements by terrorists. Keeping track of jihadi websites requires vigilance as statements and videos by individuals and groups may appear only for a short period of time. Law enforcement agencies throughout the world can learn from each other and cooperate in the fight against illicit and anti-social activities online. Indeed, there are many similarities between counterterrorism activities online and activities to counter child pornography and racism on the Internet.

Conclusion
The Internet is the single most important factor in transforming largely local concerns and activities into the broader transnational jihad. It is ubiquitous, interactive, fast and decentralized. The Internet’s ease of access, low cost, high speed, chaotic structure (or lack of structure), anonymity and international character furnish all kinds of individuals and
organizations with an easy and effective arena for their partisan interests. As the years pass, there is growing awareness of the terrorist threat online, and of the need to combat it. With concerted cooperation, capabilities to address the formidable challenges and provide appropriate answers can be developed and maintained. Indeed, to have effective results in combating terrorism, cooperation is vital.

Raphael Cohen-Almagor is Professor and Chair in Politics and Director of the Middle East Study Group, University of Hull. This article is adapted by the author from “In Internet’s way: Terrorism on the Free Highway,” published by the Jerusalem Post on 23 October 2012.