



Jihad on the information Superhighway

Raphael Cohen-Almagor

26 May 2017

The Internet has become a major arena for modern jihadis. Understanding how militant Islamist groups operate online can help security services devise appropriate methods to forestall jihadist activities.

Modern terrorism relies heavily on modern technology. Indeed, modern technology is a defining characteristic of today's terrorism. Both modern terrorism and modern technology are diffusive, decentralised, universal, interactive, low cost and chaotic in their respective structures (or lack of structures).

The Internet has enabled a global jihad based on a loose network of Mujahedeen (people who fight for jihad) transcending the limitations of face-to-face interaction. Jihadis are making the most of the vast information available on the Internet to coordinate, to communicate, and to find essential data in order to wage anti-social, violent operations.

How jihadis use the internet

Propaganda, Indoctrination and Recruitment – Most radical and terrorist organizations use the Internet as a vehicle for ideological indoctrination. There are numerous cases of normal, often non-religious citizens becoming radicalized by jihadist websites, leaving them vulnerable to terrorist recruitment. The content of such propaganda usually consists of enemy demonization, justification of violence, and a general background of the jihadi group, its platform and objectives. The sites 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. Recruiters use messaging apps like [Kik](#) to communicate with those

Latest

[An Update on the Security Policy Change Programme](#)

[Chances for Peace in the Third Decade](#)

[A Story of ORG: Oliver Ramsbotham](#)

[A Story of ORG: Gabrielle Rifkind](#)

Most read

[The Role of Youth in Peacebuilding: Challenges and Opportunities](#)

[Making Bad Economies: The Poverty of Mexican Drug](#)

who seek advice on how to cross into Syria. Terrorists proactively troll social media sites for individuals they believe may be susceptible and sympathetic to their violent messages. Indeed, Internet recruitment by ISIS is a major concern for European countries. Social media is utilised for the most anti-social activities.

Hizb ut-Tahir, an Islamist extremist group, offers music and computer games to introduce their ideology and to attract young supporters. They depict Islam as under attack, and claim Muslims have a personal duty to fight attackers. Officially, the group distances itself from violence. At the same time, Hizb ut-Tahir, in Danish propaganda leaflets, **urged** Muslims to kill Jews wherever they are. It also supports offensive jihad against Israel. People affiliated with Hizb ut-Tahir have been linked to violent acts in multiple countries, including coup attempts in the Middle East, the murder of a pro-secularist blogger in Bangladesh, and spreading anti-Western and Muslim-separatist propaganda in the West.

Al-Qaeda in the Arabian Peninsula (AQAP) publishes its English language jihadist magazine *Inspire*. The magazine, known for its high production standards, is designed to radicalize English-speaking Muslims, and encourages them to engage in militant activity. *Inspire* calls upon jihadists to mount attacks in the countries where they live. In December 2015, the Islamic State launched a cyber war magazine for jihadists called *Kybernetiq* that instructs militants about technology. The Islamic State is exploiting the Internet to the fullest, using social networks such as Facebook and Twitter to communicate with its audiences, and diversifying its reach by also using peer-to-peer apps like Telegram (fast, simple and free messaging service with enhanced security measures), Surespot (a secure mobile messaging app that uses end-to-end

Cartels

ORG's Vision

Remote Warfare: Lessons Learned from Contemporary Theatres

encryption for every text, image and voice message) and content sharing such as [JustPaste](#).

[Anwar al-Awlaki](#) was one of the iconic figures of modern terrorism. The American-Yemeni cleric was the leading English-speaking propagandist for al-Qaeda who was embraced also by the Islamic State. He was described by the FBI as the “senior recruiter for al Qaeda”. For his operational and leadership roles with al-Qaeda and for plotting attacks intended to kill Americans, al-Awlaki was killed by an American drone in 2011. But his influence endures beyond the grave.

al-Awlaki’s propaganda helped radicalize several jihadists, including the terrorist Nidal Hasan from Fort Hood, Texas who murdered 13 people and wounding 32 others in a 2009 shooting rampage; Roshonara Choudhry, a 21-year-old student who stabbed in May 2010 MP Stephen Timms because of his 2003 vote in British parliament in support of the Iraq war; Dzhokhar Tsarnaev and his brother Tamerlan Tsarnaev, the Boston Marathon bombers (April 2013) who murdered three spectators and wounded more than 260 other people; Syed Rizwan Farook and Tashfeen Malik, the San Bernardino terrorists who murdered 14 people and injured 22 others in December 2015; Elton Simpson and Nadir Soofi who aimed to kill people who attended the “Draw Muhammad” cartoon contest in Garland, Texas in May 2015; Mohammad Youssef Abdulazeez who in July 2015 murdered four US marines in attacks on two facilities in Tennessee, and Omar Mateen, who murdered 49 people and wounded 53 others in a June 2016 mass shooting at Pulse nightclub in Orlando.

Elsewhere, Hamas uses a network of websites targeting many populations. Its Website, the [Palestinian Information Center](#), appears in eight languages. It

provides propaganda and updates the Palestinian take on the news.

The military wing of Hamas, the Ezzedin al Qassam Brigades, has its own [website](#). It provides reports on current affairs, glorifies martyrs, offers interviews with Palestinians and intellectuals who support the armed struggle against Israel, provides information about their prisoners, and offers a comprehensive photo gallery. One of Hamas's Websites was designed to [target children](#): the site presented, in comic-book style, stories that encouraged children to engage in jihad and to become "martyrs".

Online jihadi propaganda can also be a potent form of psychological warfare. ISIS and Al-Qaida regularly publish videos that are designed to evoke fear. Violence plays a key role in the psyche of jihadists. The majority of videos distributed on jihadi forums feature explicit violence. On 19 April 2017 I wrote the words "ISIS violence" on YouTube search engine. The search yielded 706,000 results. The top results warned the viewers of graphic violence and of horrific ISIS executions.

Networking – The Internet can help bridge the gap from the isolated potential mujahid to the global jihad. Connection between people may start on social networking sites such as Facebook, Twitter, Telegram and Vibe and then may continue on more obscure forums. The anonymity which individuals and groups may enjoy on the Internet, the encrypted capabilities and the international character of the Internet provide terrorists with an easy and effective arena for their destructive interests.

The dark Internet is a home to illicit jihadi information and communication. 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. The forums, where people seem to care for each other, provide them with friends and support. The forums prove the existence of the ummah, or transnational Muslim community.

Fundraising – Follow the money is a good advice for those who wish to understand the world of terrorism. Terrorist groups raise funds via the Internet by five primary methods:

1. Making appeals via e-mail or directly through their websites. Hamas has circulated appeal letters to various newsgroups. Hezbollah supplied bank account information to those who solicit the group by e-mail and it posted its bank account information directly on several of its websites. The [Ibn Taymiyya Media Center \(ITMC\)](#), an online jihadist propaganda unit located in the Gaza Strip, has been using social media to run a fundraising campaign. It is one of the first terrorist groups to [publicly use](#) the digital currency bitcoin.
2. Selling goods. Many sites offer online “gift shops”: visitors can purchase or download free posters, books, videos, pictures, audiocassettes and discs, stickers, badges, symbols, and calendars.
3. Through 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. The Hezbollah had coordinated the transportation, distribution, and sale of multi-ton bulk shipments of cocaine from South America. Large cash money was [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 the Hezbollah.

4. Via 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 are legitimate front organizations which enable to raise money from across the globe. In 2013, the UK Charity Commission warned of a risk that funds raised in the name of 'charity' generally or under the name of a specific charity are misused to support terrorist activities, with or without the charity's knowledge. In 2017, the Charity Commission reported that alleged links between charities and terrorism or extremism have surged to a record high.
5. Through 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, worked for al-Qaida in Iraq. They stole money through online gambling sites. With different Trojan viruses, the three terrorists managed to raise more than 3.5 million dollars to buy web hosting services in order to show more influential videos of al-Qaida.

Spreading tactics, planning of attacks and coordination of activities –

Information technology has enabled terrorist organizations to receive and share knowledge globally. Terrorists can easily obtain information on sensitive targets and their potential weaknesses; public transport timetables; building sites, their opening times and their layout. Terrorist organisations maintain extensive databases that contain information about potential American targets.

Multiple password-protected forums refer to extensive literature on explosives. Terrorists disseminate detailed manuals how to terrorise, kill and create mayhem. There is an immense amount of how-to material: cell phone detonators, how to make flamethrowers and napalm bombs together with violent and terrorist propaganda. There are detailed tutorials in 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.

There is strong *evidence* that such online instructions played a critical role in the March 2004 Madrid bombings, the April 2005 Khan al-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. The information help radical so-called "lone-wolfs" (who, thanks to the Internet, are never alone) to plan their actions.

The Internet has proven to be an excellent vehicle by which information about travel, training, targets, tactics and a host of other useful organization details is displayed. Data, instructions, maps, diagrams, photographs, tactical and technical details are often sent in this exchange, often in encrypted format, using onion routers such as Tor that hide the Internet Protocol (IP) address. Gilles de Kerchove, EU Counter-terrorism Coordinator, said: *"We have to be vigilant, since the threat posed by the so-called Islamic State (IS) and returning foreign fighters is likely to persist in the coming years"*.

Al-Qaida members used the Internet in planning and coordinating the attacks of September 11, 2001. Mary E. Galligan, FBI Chief Inspector who supervised PENTTBOM, the FBI's investigation of the attacks, studied closely the incident

that brought about the global war on terror. She said that clearly the Internet was a vital channel for coordination of those attacks. Galligan asserted that al-Qaida terrorists learned the methods used by the US to combat terrorism; they studied the American soft spots and targets.

Al-Qaida activists 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. Al-Qaida activists were looking for American flight schools on the Internet, while they were in Germany.

The terrorists used public libraries 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 September 11, some of which included operational details of the planned terrorist assault.

In 2015, Sid Ahmed Ghulam tried to open fire on a church in Paris. When the police searched his car, they found in his laptop a series of messages showing how he had been guided by a pair of handlers who provided both the weapons and the getaway car. Ghalem was remote-controlled by his handlers with the help of technology.

The Telegram platform which enables end-to-end encryption was used by terrorists before the attacks on Nice in July 2016 and Berlin in December 2016. It is believed that videos of high profile attacks were posted on Telegram by jihadists to inspire and motivate each other, including the murder of soldier Lee Rigby in Woolwich and the 7/7 London bombings.

In March 2017, Khalid Masood launched a terror attack near the British Houses of Parliament in which four people died and more than 35 others were injured. Minutes before the attack, Masood communicated with other people via the WhatsApp platform. WhatsApp, owned by Facebook, uses end-to-end encryption which prevents even its own technicians from reading people's messages. This makes the work of law enforcement agencies particularly difficult.

Responding to the cyber-jihad

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 counter-online terrorism activities, counter-online child-pornography activities and counter-online racism activities. To have effective results in fighting down terrorism, cooperation is vital. Failure to do so is inexcusable.

Without responsible cooperation, Internet abusers will prevail, and our children will suffer. Nations, Internet intermediaries and responsible Netcitizens are obliged to ensure that future generations will be able to develop their autonomy, their individuality and their capabilities in a secure environment, both offline and online.

Image credit: Pixabay

Raphael Cohen-Almagor received his DPhil in political theory from Oxford University. He is Professor/Chair in Politics, and Founder and Director of the Middle East Study Group, University of Hull, UK. He is the author of hundreds of publications in politics, law, media and ethics, including most

recently *Confronting the Internet's Dark Side* (NY and Washington DC.: Woodrow Wilson Center Press and Cambridge University Press, 2015), the first comprehensive book on social responsibility on the Internet. <https://www.wilsoncenter.org/book/confronting-the-internets-dark-side-moral-and-social-responsibility-the-free-highway>. Website: <http://www.hull.ac.uk/rca>. Blog: <http://almagor.blogspot.com> Twitter: @almagor35

Share this page



Contact

Unit 503
101 Clerkenwell Road London
EC1R 5BX
Charity no. 299436
Company no. 2260840

Email us

020 3559 6745

Follow us



Registered with
**FUNDRAISING
REGULATOR**

Useful links

[Login](#)
[Contact us](#)
[Sitemap](#)
[Accessibility](#)
[Terms & Conditions](#)
[Privacy policy](#)