

# Terror on Facebook, Twitter, and Youtube

---

GABRIEL WEIMANN

Professor

Haifa University

---

“MY DEAR BROTHERS IN JIHAD,” wrote a man who identified himself as Abu Jendal, “I have a kilo of Acetone Peroxide. I want to know how to make a bomb from it in order to blow up an army jeep; I await your quick response.” About an hour later the answer came: “My dear brother Abu Jendal,” answered a Hamas supporter who called himself Abu Hadafa, “I understand that you have 1,000 grams of *Om El Abad*. Well done! There are several ways to change it into a bomb.” *Om El Abad*—the mother of Abad—is the Hamas nickname for the improvised explosive TATP—triacetone triperoxide. Abu Hadafa then explained, in detail, how to change the homemade explosive into a deadly roadside bomb, and even attached a file that teaches how to make detonators for the bomb.<sup>1</sup> Abu Jendal and Abu Hadafa are two anonymous Palestinians who, it seems, never met one another. The exchange was not encoded or concealed, but was published completely openly on the website of the *Izz al din al Kassam* Brigades, the military faction of the Hamas.

This online form of exchanging of guidance, advice, and instructions has become commonplace in various terrorist chatrooms and online forums. Post-modern terrorists are taking advantage of the fruits of globalization and modern technology—especially advanced online communication technologies that are used to plan, coordinate and execute their deadly campaigns. No longer geographically constrained within a particular territory, or politically or financially dependent on a particular state, they rely on technologically modern forms of communication—including the internet. The internet has long been a favorite tool for terrorists.<sup>2</sup> Decentralized and providing almost perfect anonymity, it cannot be subjected to controls or restrictions, and can

---

GABRIEL WEIMANN is Professor of Communications at Haifa University and The School of International Studies at American University. He is author of multiple books including *Terror on the Internet: The New Arena, the New Challenges* (2006), *The Singaporean Engima* (2001) and *Communicating Unreality: Mass Media and Reconstruction of Realities* (2000).

---

Copyright © 2010 by the *Brown Journal of World Affairs*

be accessed by anyone. The internet has enabled terrorist organizations to research and coordinate attacks; to expand the reach of their propaganda to a global audience; to recruit adherents; to communicate with international supporters and ethnic diasporas; to solicit donations; and to foster public awareness and sympathy for their causes. The internet also allows terrorists to convey their messages to international and distant audiences with whom it would otherwise be difficult to communicate. The internet provides a means for terrorist groups to feed the mass media with information and videos that explain their mission and vision. By these means, the group's message can reach a greater audience and more easily influence the public agenda.<sup>3</sup>

In addition to launching their own websites, terrorists can harness the interactive capabilities of chatrooms, instant messenger, blogs, video-sharing websites, self-determined online communities, and social networks. As Noguchi and Kholmann found, "90 percent of terrorist activity on the internet takes place using social networking tools, be it independent bulletin boards, Paltalk, or Yahoo! eGroups. These forums act as a virtual firewall to help safeguard the identities of those who participate, and they offer subscribers a chance to make direct contact with terrorist representatives, to ask questions, and even to contribute and help out the cyber-jihad."<sup>4</sup>

By now, all active terrorist groups have established at least one form of presence on the internet and most of them are using all formats of modern online platforms, including e-mail, chatrooms, e-groups, forums, virtual message boards, and resources like You-Tube, Facebook, Twitter, and Google Earth. This essay examines the use of interactive online communication by terrorists and their supporters—from chatrooms to Twitter and Facebook.

## TERRORIST CHATROOMS

Chatrooms and electronic forums enable terrorist groups to communicate with members and supporters all over the world, to recruit new followers and to share information at little risk of identification by authorities. The free chatroom service PalTalk, which includes voice and video capabilities, has become particularly popular with terrorist cells. In one PalTalk chat room, British Islamic militants were found to have set up support forums for the killed leader of the insurgents in Iraq, Abu Musab al-Zarqawi. In another chatroom, Arabic-speaking users shared personal experiences of fighting Arab-Afghans. In another, relatives of Iraqi insurgents praised the "martyrdom" of the terrorists.<sup>5</sup> On the alneda.com forum, al-Qaeda members posted comments praising Osama Bin Laden, such as "Oh Allah! Support your fighting slave Osama bin Laden." Other message boards included threats against global security and reference to the 2005 London bombings. The website and forum were infiltrated and closed down by

an American hacker, but that did not stop al-Qaeda members, who simply started a new forum.

In addition to generating support, terrorist groups use chatrooms to share tactical information. Jihadist message boards and chatrooms have been known to have “experts” directly answer questions about how to mix poisons for chemical attacks, how to ambush soldiers, how to carry out suicide attacks and how to hack into computer systems. One chatroom on the PalTalk index, with a name that is slightly altered each time but still identifiable, has been routinely advertised on Jihadi web forums and has been used on a daily basis to post links to al-Qaeda propaganda videos and terrorist instruction manuals.<sup>6</sup> The forums Qalah, Al-Shamikh, Majahden, and Al-Faloja are especially popular among terrorist cells, and new recruits are encouraged to refer to the sites to read the jihadist literature. These chatrooms also aim to convince prospective members to join or to stage personal suicide attacks.

According to SITE’s special report on Western Jihadist Forums, during 2009 several notable technical changes occurred in many of the jihadist forums.<sup>7</sup> For example, the long offline, prominent English-language jihadist forum, al-Firdaws English, returned on 24 May 2009 in a form that is open to the public, rather than password-protected. Permitting non-members to view discussion and content on the forum is a significant departure for al-Firdaws style, as previous iterations of the forum have been both completely password-protected and not open to new membership. The forum administration’s decision to open the forum to public observation suggests that they may envision the forum containing less sensitive information in the future. Despite allowing forum visitors to access threads and read content, al-Firdaws English remains closed to new and prospective members.

The case of Younes Tsouli is especially demonstrative of the resourceful uses of the internet by terrorists. As one journalist put it, Tsouli, more commonly known by his internet pseudonym “Irhabi 007,” “illustrated perfectly how terrorists are using the internet not just to spread propaganda, but to organize attacks.”<sup>8</sup> Between 2003 and the time of his arrest in December 2007, Irhabi

**The case of Younes Tsouli is especially demonstrative of the resourceful uses of the internet by terrorists.**

007 engaged in several instrumental activities on the internet. In 2003, he began joining various terrorist internet forums, where he uploaded and published pictures, videos, and instruction manuals on computer hacking. Shortly thereafter his skills were sought out by al-Qaeda leaders who wanted him to provide logistical support for their online operations, and in 2005 Tsouli became the administrator of the extremist internet forum al-Ansar, where he began publishing bomb making instruction manuals and details related to suicide bombing operations. He helped Zarqawi’s al-Qaeda faction in

Iraq and became a central figure in enabling Zarqawi to reestablish the links between al-Qaeda affiliated groups after the fall of the Taliban. Irhabi 007 eventually hacked his way into an unprotected file directory on an Arkansas state government website. He then posted propaganda and beheading videos. Cyber-tracking intelligence immediately noticed Irhabi 007's perfect English and questioned the cybercriminal's nationality. Younis Tsouli was caught in 2006. On his home computer, British investigators found photos of locations in Washington D.C. that had been emailed to him by colleagues which suggested that he was helping to organize a terrorist attack on Capitol Hill. Of course, after Tsouli was caught, other cyberterrorists learned from his mistake.

### WHEN TERRORISTS "TWEET"

48 An intelligence report released in October of 2008 by the U.S. Army's 304<sup>th</sup> Military Intelligence Battalion included a chapter entitled the "Potential for Terrorist Use of Twitter," which expressed the Army's concern over the use of the blogging service.<sup>9</sup> The report says that Twitter could become an effective coordination tool for terrorists trying to launch militant attacks. The Army report includes references to several pro-Hezbollah tweets. The report also highlights three possible scenarios of terrorist use of Twitter. The first scenario is that terrorists can send and receive near real-time updates on the logistics of troop movements in order to conduct more successful ambushes. In the second, one operative with an explosive device or suicide belt could use his mobile phone to send images of his or her location to a second operative who can use the near real-time imagery to time the precise moment to detonate the explosive device. The third is that a cyberterrorist operative could find and compromise a soldier's account and communicate with other soldiers under the stolen identity.<sup>10</sup> Although the last two options seem a bit far-fetched and difficult for terrorists to carry out successfully, the first option is a very viable threat. The instantaneous update capabilities could help the terrorists organize more precise and detrimental ambushes.

According to the SITE report, despite the potential utility of Twitter, members of terrorist groups continue to be wary of networking sites such as Facebook. In response to a forum member's suggestion to become friends on Facebook, some Ansar al-Mujahideen posters envisioned that such a network of friends could be a danger to Western jihadists. In a thread begun on 4 May 2009, Ansar al-Mujahideen members attempted to dissuade a member (called "islamic jihad union") from connecting with other jihad supporters on Facebook. Soon, other Ansar al-Mujahideen participants were warning against using Facebook. Several forum members opined that the risks of having their real identity tied to their online personas outweighed the potential gains from networking with other jihad supporters.

## **SOCIAL NETWORKING**

Popular social networking websites are another means of attracting potential members and followers. These types of virtual communities are growing increasingly popular all over the world, especially among younger demographics. Jihadist terrorist groups especially target youth for propaganda, incitement, and recruitment purposes. Terrorist groups and their sympathizers are using predominately Western online communities like Facebook, MySpace, Second Life, and their Arabic equivalents more frequently. Counter-terrorism expert Anthony Bergin says that terrorists use these youth-dominated websites as recruitment tools, “in the same way a pedophile might look at those sites to potentially groom would-be victims.”<sup>11</sup>

Social networking websites allow terrorists to disseminate propaganda to an impressionable age bracket that might empathize with their cause and possibly agree to join. Many users join interest groups that may help terrorists target users they might be able to manipulate. Many social network users accept people as friends whether or not they know them, thereby giving perfect strangers access to personal information and photos. Some people even communicate with the strangers and establish virtual friendships. Terrorists apply the narrowcasting strategy to social networking sites as well. The name, accompanying default image, and information on a group message board are all tailored to fit the profile of a particular social group. The groups also provide terrorists with a list of predisposed recruits or sympathizers. In the same way that marketing groups can view a member's information to decide which products to target to a webpage, terrorist groups can view people's profiles to decide whom they are going to target and how they should configure the message.

Yet, terrorists are well aware of the risks involved. A member of a Jihadi forum in English issued a warning, reminding readers that a Facebook network would allow security agencies to trace entire groups of jihadists, arguing:

Don't make a network in Facebook...Then Kuffar will know every friend you have or had in the past. They will know location, how you look, what you like, they will know everything! Join Facebook if you want and use it to keep in touch with friends and brothers far away but not as a network.<sup>12</sup>

As a strategy to distribute jihadist propaganda to a wide range of Muslims and overcome countermeasures, a posting on the al-Fallujah jihadist forum on 16 March 2009 suggested that administrators of similar forums and media organizations create e-mail groups. This mailing group is patterned after the Ansar Mailing Group, an inactive jihadist media distributor that dispatched news of the mujahideen to users via e-mail. He suggested that other jihadists, too, create such groups to reach the largest possible

number of users, and that they should remove any obstacle in the registration process that hinders distribution. To this end, the jihadist, in a later posting, provided instructions for creating groups on Google. Another forum participant, pleased with the suggestion, gave instructions on how to create a user account on Yahoo, and added that groups may be created on that service.

#### **YOU HAVE A FRIEND REQUEST: FACEBOOK**

Membership within the international Facebook community has boomed in recent years. Facebook is currently the world's most popular social networking website with an estimated 222 million users world wide, which includes a 66 percent membership increase within the Middle East and a 23 percent increase in Asia.<sup>13</sup> Terrorists have taken note of the trend and have set up profiles as well. There are numerous Facebook groups declaring support for paramilitary and nationalist groups that the U.S. government has designated as terrorist organizations, such as Hezbollah, Hamas, the Turkish Revolutionary People's Liberation Army, and the Liberation Tigers of Tamil Eelam (LTTE). The majority of these groups have open pages and anyone interested can read the information, look at the discussion boards, click on links to propaganda videos, and join the group.

50

Deputy Director for Intelligence at the National Counterterrorism Center Andrew Liepmann recently reported to Congress that the Federal Bureau of Investigations is tracking a few Somali-Americans from the Minneapolis area that were reportedly recruited for the purpose of starting a U.S. terrorist cell of the Al-Shabaab faction through Facebook.<sup>14</sup> The FBI is keeping a close eye on one Facebook user who posted a photo of a man wearing a black mask over his face and holding what appears to be the Koran in one hand and a grenade launcher in the other. Although some might argue that the aforementioned posting is probably in violation of Facebook's terms of use, which bans posting "threatening," "harassing," or "hateful" messages, the FBI is finding it difficult to regulate terrorist activity on the internet because of First Amendment right issues. It is also nearly impossible to track down individuals involved in these sorts of instances because of the international nature of the websites. Social networking websites do not always have identifiable information about users; all that is needed to register for the websites is an email address and users often set up their accounts under false names and details.

Terrorists can use these social networking sites to monitor military personnel. In 2008, the Canadian Defense Department and the British Secret Service M15 requested that troops remove personal details from social networking sites because of alleged monitoring by al-Qaeda operatives. U.S. personnel are also warned against

posting certain details or photos on their profile pages. Even if the information does not give details about the logistics of troop movements, it could potentially endanger the friends and relatives of military and security personnel. Many soldiers unwittingly post detailed information about themselves, their careers, family members, date of birth, present locations, and photos of colleagues and weaponry. Canadian troops have been asked to exclude any information from their profiles that might even link them with the military. A report from the Lebanese capital of Beirut later that year stated that Hezbollah had been monitoring Facebook to find potentially sensitive information about Israeli military movements and intelligence that could be harmful to the national security of Israel. The report quoted an Israeli intelligence official saying that “Facebook is a major resource for terrorists, seeking to gather information on soldiers and IDF [Israel Defense Forces] units and the fear is soldiers might even unknowingly arrange to meet an internet companion who in reality is a terrorist.”<sup>15</sup>

According to a posting on al-Ekhlaas, a password-protected al-Qaeda affiliated forum dated 21 August 2008, a group for supporters of the Islamic State of Iraq (ISI) and al-Qaeda is also using Facebook.<sup>16</sup> The post briefly describes the pictures found in this Facebook group, which include shots of Osama bin Laden, Ayman al-Zawahiri, and ISI mujahedeen. One of the members commented on the utility of such a group: “these sites can be exploited to post our ideas and what we owe Allah to those who do not carry our ideology.”

## **YOUTUBE AND “THEYTUBE”**

YouTube was established in February 2005 as an online repository facilitating the sharing of video content. YouTube claims to be the “the world’s most popular online video community.” A 2007 report from the Pew Internet and American Life Project put the percentage of U.S. online video viewers using YouTube at 27 percent, ahead of all other video sharing sites. In the 18 to 29 year-old age demographics, YouTube’s leadership is even more pronounced, with 49 percent of U.S. online video viewers. In fact, *CNNMoney* reported that in January 2008 alone, nearly 79 million users worldwide viewed more than three billion YouTube videos.

Terrorist groups realized the potential of this easily accessed platform for the dissemination of their propaganda and radicalization videos. Terrorists themselves have praised the usefulness of this new online apparatus: “A lot of the funding that the brothers are getting is coming because of the videos. Imagine how many have gone after seeing the videos. Imagine how many have become shahid [martyrs],” convicted terrorist Younis Tsouli (so-called “Ithabi007”) testified. In 2008, jihadists suggested a “YouTube Invasion” to support jihadist media and the administrators of al-Fajr-affili-



ated forums.<sup>17</sup> This suggestion was posted on al-Faloja, a password-protected jihadist forum, on 25 November 2008. The posting provides a synopsis of the YouTube site and its founding, and notes its use by, among others, President Barack Obama during his presidential campaign. YouTube is argued to be an alternative to television as a medium that allows for jihadists to reach massive, global audiences. This particular message even instructs jihadists to cut mujahedeen videos into ten-minute chunks, as per YouTube's requirements, and upload them sequentially to the site. "I ask you, by Allah, as soon as you read this subject, to start recording on YouTube, and to start cutting and uploading and posting clips on the jihadist, Islamic, and general forums," said the poster. "Shame the Crusaders by publishing videos showing their losses, which they hid for a long time."

Hezbollah, Hamas, the LTTE and the Shining Path of Peru all have propaganda videos on YouTube. One LTTE YouTube user has posted over 100 videos in 2009 alone.<sup>18</sup> In 2008, Hamas allegedly launched its own video-sharing website, although the group denied ownership of the site. AqsaTube, in addition to choosing a similar name, was designed to look just like YouTube and even copied its logo. Once certain internet providers refused to host the website, Hamas launched a PaluTube and TubeZik.<sup>19</sup> The LTTE has also launched TamilTube.<sup>20</sup> These videos are not just aimed at Middle Eastern Muslim youths. More recent videos posted on these video-sharing websites are dubbed in English or have English subtitles.


A recent study conducted by Conway and McInerney analyzed the online supporters of jihad-promoting video content on YouTube, focusing on those posting and commenting upon martyr-promoting material from Iraq.<sup>21</sup> The findings suggest that a majority are less than 35 years of age and reside outside the region of the Middle East and North Africa with the largest percentage of supporters located in the United States. As the researchers concluded: "What is clearly evident however is that jihadist content is spreading far beyond traditional jihadist websites or even dedicated forums to embrace, in particular, video sharing and social networking—both hallmarks of Web 2.0—and thus extending their reach far beyond what may be conceived as their core support base in the Middle East and North Africa region to Diaspora populations, converts, and political sympathizers."

## CONCLUSION

Much of the original online terrorist content was one-directional and text-based, either in the form of traditional websites with a heavy reliance on text or as messages posted on forums. However, technological advances, particularly the increased availability of sophisticated, but cheap and user-friendly video capturing hardware (e.g., hand-held



digital video cameras, mobile telephones, etc.) and interactive online networking platforms (e.g., Facebook) have changed terrorist online communications. The global community created by social networks and interactive forums on the internet is advancing cultural awareness and reconciliation efforts, but it is also advancing terrorists' goals to share their extremist messages to global audiences. By using these online communities to their advantage, not only can terrorists promote global paranoia, share their messages with sympathizers, and obtain donations, but they can also create more terrorists. The internet has provided terrorists with a whole new virtual realm to conduct their sinister back-alley transactions. Terrorist groups are no longer confined to specific regional boundaries—now terrorist networks can recruit and members located in any part of the globe.<sup>22</sup> A person in the United States can literally take a terrorist training course within the privacy of their bedroom.

The interactive capabilities of the internet, like chatrooms, social networking sites, video-sharing sites and online communities, allow terrorists to assume an offensive position. Instead of waiting for web-surfers to come across their websites and propaganda materials, terrorists can now lure targeted individuals to the sites. Paradoxically, the most innovative network of communication developed by the West with its numerous online networking platforms now serves the interests of the greatest foe of the West, international terrorism. 

## NOTES

1. This exchange was reported by Amit Cohen, " Hamas Dot Com", in *Maariv Online*, 7 February 2003.

2. Gabriel Weimann, "How Modern Terrorism Uses the Internet," United States Institute of Peace Special Report 116 (2004), <http://www.usip.org/pubs/specialreports/sr116.pdf>; Gabriel Weimann, *Terror on the Internet: The New Arena, The New Challenges*. (Washington, DC.: USIP Press Books, 2006a); Gabriel Weimann, "Virtual Training Camps: Terrorist Use of the Internet," in ed. James Forest *Teaching Terror: Strategic and Tactical Learning in the Terrorist World* (Boulder: Rowman & Littlefield Publishers, 2006b): 110-132.

3. David H. Gray, and Albon Head. "The Importance of the Internet to the Post- Modern Terrorist and its Role as a Form of Safe Haven." *European Journal of Scientific Research* 25 (2009): 396-404.

4. Yuki Noguchi, and Evan Kholmman. "Tracking Terrorists Online." Washingtonpost.com video report. 19 April 2006. *The Washington Post*, <<http://www.washingtonpost.com/wp-dyn/content/discussion/2006/04/11/DI2006041100626.html>>, accessed 11 March 2009 .

5. Evan Kholmman, "Al Qaeda and the Internet." *Washingtonpost.com* video report. The Washington Post, accessed 2 August 2005.

6. Elizabeth Montalbano, "Social networks link terrorists." *Computer World*, 7 January 2009, accessed 13 March 2009.

7. *InSITE*: Western Jihadist Forums: The Monthly SITE Monitoring Service on Western Language Jihadist Websites, April-May 2009, accessed June 2009.

8. Gordon Corera, "Al-Qaeda's 007: The Extraordinary Story of the Solitary Computer Geek in a Shepherd's Bush Bedsit Who Became the World's Most Wanted Cyber-Jihadist," *Times Online*, 16 January 2008, [http://women.timesonline.co.uk/tol/life\\_and\\_style/women/the\\_way\\_we\\_live/article3191517.ece](http://women.timesonline.co.uk/tol/life_and_style/women/the_way_we_live/article3191517.ece).

9. "U.S. Army Says Blogging Site 'Twitter' Could Become Terrorist Tool." *Fox News*, 27 October 2008, accessed 11 March 2009.
10. Noah Shachtman, "Spy Fears: Twitter Terrorists, Cell Phone Jihadists." *Wired*, 24 October 2008, accessed 8 March 2009.
11. "Facebook terrorism investigation." *The Advertiser*, 5 April 2008, accessed 10 March 2009.
12. *InSITE*: "Western Jihadist Forums," *ibid*.
13. "Social Networking Explodes Worldwide as Sites Increase their Focus on Cultural Relevance." Press release. *ComScore.com*. 12 August 2008, accessed 15 March 2009.
14. Andrew Liepman, Violent Islamist Extremism: Al-Shabaab Recruitment in America. Hearing before the Senate Homeland Security and Governmental Affairs Committee, 11 March 2009.
15. "Cyber Terrorism: Perils of the Internet's Social Networks." *Middle East Times* [Washington D.C.] 8 September 2008.
16. *InSITE*, "ISI Supporters Group on Facebook," 21 August 2008.
17. "Jihadist Forum Suggests YouTube Invasion," *The Telegraph*, 4 December 2008, <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3547072/Jihadist-forum-calls-for-YouTube-Invasion.html>.
18. <http://www.youtube.com/user/TamilEelamTigers>.
19. The Internet and Terrorism: Hamas and Palutube "Global Terrorism." *Right Side News*, 6 April 2009.
20. <http://www.tubetamil.com>.
21. Maura Conway and Lisa McInerney, 2008. "Jihadi Video & Auto-Radicalisation: Evidence from an Exploratory YouTube Study," In Proceedings of the 1st European Conference on intelligence and Security informatics, Esbjerg, 3-5 December 2008.
22. Maura Conway, "Terrorism and the Internet: New Media- New Threat?" *Parliamentary Affairs* 59 (2006): 283-98.

Copyright of Brown Journal of World Affairs is the property of Brown University and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.