ABSTRACT

The article is opened with definitions of terms utilized throughout the article. Terrorism is defined as the threat or employment of violence against noncombatant targets for political, religious, or ideological purposes by sub-national groups and/or clandestine individuals who are willing to justify all means to achieve their goals. Terrorist conduct is designed to attract attention to the terrorist’s cause and to spread fear and anxiety among wide circles of the targeted population. Subsequently the author analyses how terrorists use the Internet, and what can be done to counter their activities. The Internet is used to disseminate information, for propaganda, indoctrination, networking, psychological warfare, socialization, motivation, fund raising, spreading tactics, recruitment, planning activities and coordination. As the Internet became a major arena for modern terrorists, we need to devise appropriate methods to forestall their activities and establish security.

Keywords: Al-Qaeda, Counter-Terrorism, E-Jihad, Encryption, Jihad, Terror

1. INTRODUCTION

The aim of this article is to analyse the ways radical, terrorist Islamists exploit the Internet, and what can be done to counter their activities. It is opened by definitions of terrorism, cyberterrorism and e-jihad. This section also provides background material about al-Qaeda and about technology designed to protect one’s anonymity and privacy which is conveniently abused by terrorists: Encryption and onion routers. Section III explains how terrorists are using the Internet. Modern terrorism is diffused into cells in different parts of the world. The Internet plays a crucial part in maintaining connections between those cells. Indeed the Internet is a great socialization tool. It brings together like-minded people and creates a forum to discuss and exchange ideas. The Internet has been used to deliver instructions and plans, to coordinate and prepare violent operations against designated targets (Atwan, 2006, p. 124).

There are obvious similarities between the Internet and modern terrorism. Both the Internet and the jihadist movement are diffused and decentralized; both are lacking a coherent structure; both are global and quite chaotic. Section IV details the appropriate countermeasures. The threat of terrorism is real and significant. As the Internet became a major

DOI: 10.4018/ijcwt.2012070104
arena for modern terrorists, we need to devise appropriate methods to forestall their activities and establish security.

2. DEFINITIONS AND BACKGROUND INFORMATION

The word “terror” comes from the Latin “terrere,” meaning “to frighten” or “to scare” (Matusitz, 2013, p. 1). For the purposes of this study, terrorism is defined as the threat or employment of violence against noncombatant targets for political, religious, or ideological purposes by sub-national groups and/or clandestine individuals who are willing to justify all means to achieve their goals. Terrorist conduct is designed to attract attention to the terrorist’s cause and to spread fear and anxiety among wide circles of the targeted population (Cohen-Almagor, 2005).1 Terrorism is usually the work of a small number of committed individuals who strive for what they perceive as the “greater good” of a larger group with whom the terrorists identify.

The Office of the Coordinator for Counterterrorism (2011) in the US State Department (S/CT) continually monitors the activities of terrorist groups active around the world. In May 2011, it listed 48 terrorist organizations. More than 30 of them were established by radical, terrorist Islamic groups. The majority of those terrorist groups use the Internet as a primary tool for their activities. The number of pro-terrorism websites is estimated to have increased from approximately 12 in 1998 to more than 4,700 by 2005 (Ariza, 2005). These websites use slogans to catch attention, often offering items for sale (such as T-shirts, badges, flags, and video or audio cassettes). Frequently the websites are designed to draw local supporters, providing information in a local language about the activities of a local cell as well as those of the larger organization. The website is, thus, a recruiting tool as well as a basic educational link for local sympathizers and supporters (Neville-Jones, 2011; Forest, 2006).

Cyberterrorism is a particular form of terrorism conducted by information technology. It is defined as ideologically-politically motivated attacks against information infrastructures which result in violence against government agencies and officials as well as noncombatant targets. Such criminal acts through computers are perpetrated by sub-national groups and clandestine agents may result in death and/or destruction, creating terror for the purpose of coercing governments to change their policies. Cyberterrorism can potentially undermine a country’s economy by attacking the critical infrastructure of major cities as dams, nuclear reactors, water and power supplies are operating via computers. Banks and other financial institutions might also be crippled by such attacks (Janczewski & Colarik, 2008).

The term E-jihad refers to the way information technology is applied by groups such as al-Qaeda in order to organize logistics for their campaigns, through the application of email and encrypted files, as well as a means for developing their own strategic intelligence (Bunt, 2003, p. 26).

As terror is perceived to be a dangerous threat to the free world, jihadists must resort to clandestine methods to promote their violent ends. Technology is instrumental in hiding web activities. Most Internet communications including email, messaging, discussion groups and web browsing can be hidden. Encryption is a method that protects the communications channel from sniffers. Encryption is based on the science of cryptography (“secret writing”) which has been used for many centuries particularly for military purposes. Encryption is used to hide the speaker’s words from the eyes of others by creating a private language between the speaker and the listener. It is a means for securing critical infrastructure and for protecting sensitive information. Once data is encrypted, the transmitted message appears in an unreadable format. Also, for decoding simple messages one needs to have some background information in order to understand the context.
Law enforcement may figure what is written, but without knowing the context, the message will be meaningless. For instance, what does it mean “On the 4th deliver four books to Jim and speak to Carole about the proof-reading”?

A further tool to protect privacy is Tor. Tor was originally designed by the US Naval Research Laboratory in order to protect government sensitive communication (“Tor: Overview,” Tor, torproject.org/about/overview.html.en). Later Tor was adopted by journalists, human rights activists, hackers, law enforcement officers and ordinary people. Presently it is the most popular onion router. It is software and an open network that helps Netusers defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. Tor is comprised of a software that can be downloaded for free, and a volunteer network of computers that enables the operation of the software (“What is a Tor Relay?,” Electronic Frontier Foundation, https://www.eff.org/torchallenge/what-is-tor). Tor protects one’s identity by bouncing one’s communications around a distributed network of relays run by volunteers all around the world. It prevents somebody watching your Internet connection from learning what sites you visit, and it protects your physical location. When you use the Tor software, your real IP address remains hidden.

3. INTERNET IN SERVICE OF RADICAL, TERRORIST ISLAMISTS

The Internet has enabled a global jihad based on a loose, decentralized network of Mujahideen transcending the limitations of face-to-face interaction (Sageman, 2004, p. 159). E-mail is as popular among radicals and terrorists as it is among other Netusers. Terrorists, like people who use the Internet for social purposes, are making the most of the vast information available on the Internet to coordinate, to communicate, to find essential data in order to wage anti-social, violent operations.

Most jihadi websites have several sections (see Figure 1 for Palestinian Islamic Jihad symbol on websites). Most important is usually the religious section, which features Quranic references to jihad, the different ways jihad can be expressed, aspects of martyrdom, fatwa (singular is fatwa, a religious edict provided by a Muslim sage) explaining who can be targeted legitimately, and online doctrinal consultations with religious sages. In the jihad section, would-be recruits are encouraged to join the battle. Some general advice is given, e.g., the best routes into war zones as well as names and locations of sympathetic mosques. Galleries of martyr portraits are accompanied by their last testaments, often in a video clip. Most sites have IT section where contributors

---

Figure 1. Palestinian Islamic Jihad symbol
are urged to share their knowledge and develop new ways of using cyberspace to further jihad. Bulletin boards and chatrooms are very popular among jihadi Netusers (interviews with Daniel Castro, Information Technology and Innovation Foundation, and with Brian Marcus, former Anti-Defamation League [ADL] Director of Internet Monitoring, Washington, DC, May 9, 2008 and June 5, 2008; Atwan, 2006, p. 141; Forest, 2006, p. xii). It is very easy to create private chatrooms on which Netusers post messages for friends and colleagues. One may advise them which chatroom to use and then interact freely. Communication can be made from any Internet cafe in the world. Interactive technology enables visitors to add comments and reply to ongoing discussions.

Many 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 (Atwan, 2006, pp. 141-142). Some show women mourn their dead loved ones.

3.1. Information

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. The Internet can be used to disclose code names and radio frequencies used by security services. Hamas was said to use Google Earth to plan its violent operations (Tamimi, 2007, p. 104; Wade and Mljevic, 2011, p. 74). Al-Qaeda maintains a database that contains information about potential American targets. This information enables them to predict the impact of an attack on a target in terms of human lives and structural damage (Thornton, 2010, p. 2). The online Minbar at-Tawhid wa-1-jihad is a library of jihadi scholarly materials.

Terrorists use the Internet to provide pictures, directions, instructions, diagrams and maps. An al-Qaeda laptop was found with information regarding the French Anonymous Society which published a book on anti-surveillance methods and information on planning assassinations (Conway, 2005, p. 17; Conway, 2006, pp. 283-298).

Hamas uses a network of websites targeting many populations. Its official Website, the Palestinian Information Center (www.palestine-info.com), appears in eight languages. It provides propaganda and updates the Palestinian take on the news.

3.2. Propaganda and Indoctrination

Most radical and terrorist organizations use the Internet as a vehicle for ideological indoctrination. Hizb ut-Tahrir (http://www.hizbut-tahrir.info/info/english.php/category_en/categ_415), an Islamist extremist group, and the Hezbollah (http://almashriq.hiof.no/lebanon/300/320/324/324.2/hizballah/), offer music and computer games to introduce their ideology and to attract young supporters. Thousands of websites and bulletin boards present audio and video material designed to promote the jihadi cause. As Islam is under attack, Muslims have a personal duty to fight. Thus, for instance, a first-person perspective computer game called Night of Capturing Bush was released to jihadist forums in September 2006 by the Global Islamic Media Front. The game features six-levels, culminating in a gun battle with President George W. Bush (http://thepiratebay.org/torrent/3526673/Night_Of_Bush_Capturing_(Terrorist_Recruiting_FPS)). YouTube hosts a number of jihadi rap video clips whose catchy, melodic message is war against the infidels and crusaders. jihad Dirty Kuffar (http://www.youtube.com/watch?v=pWZd088e2Lg; http://www.youtube.com/watch?v=sbxMmrPbz98, http://www.spike.com/video-clips/c44evm/dirty-kuffar; http://video.google.co.uk/videoplay?docid=9083681522527526242) entertains violent images with jihadi slogans and the Nazi swastika. This clip has been downloaded onto millions of computers and remixed by many jihadists (El Akkad, 2007, p. F1; Hall, 2007, p. 1A). Harakat al-Shabaab al-Mujahideen,
Al-Qaeda’s army in Somalia, tweets its #JihadDispatches on recent battles (Zelin, 2013, p. 1). There is also an immense amount of how-to material: cell phone detonators, how to make flamethrowers and napalm bombs together with violent and terrorist propaganda (Kotenko, 2013).

Al-Qaeda’s network has been successful in its use of multimedia propaganda, producing pre-recorded videotapes and audiotapes, CD-ROMs, DVDs, photographs, and written documents. Islamist zealots are developing computer games and promoting hip-hop artists in order to spread radical ideology and to reach sympathizers within adversarial populations (Forest, 2006, p. 12). 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.

Mustafa Setmariam Nasar was one of al-Qaeda’s most influential figures. His lectures were gathered in a 1,600 page publication under the title “The Call for a Global Islamic Resistance” (http://www.archive.org/details/TheGlobalIslamicResistanceCall), which was widely disseminated on the Internet in 2004. Until his arrest in 2005, Nasar appeared regularly on Islamist forums, preaching violent jihad against the west, pressing for a more decentralized and hard-line jihad, one that will resort to weapons of mass destruction. He enjoyed credibility and instructing recruits on the use of such weapons at the Derunta training camp in Afghanistan (Cruickshank and Hage Ali, 2006, p. B02; Whitlock, 2006).

In March 2011, al-Qaeda in the Arabian Peninsula (AQAP) published the fifth edition of its English language jihadist magazine Inspire (http://publicintelligence.net/inspire-al-qaeda-in-the-arabian-peninsula-magazine-issue-5-march-2011/). In July 2011, it published its sixth edition following the killing of Osama bin Laden. While the cover story was dedicated to the leader’s death and his legacy, the magazine offered detailed instructions on the production and preparation of Acetone Peroxide explosive and on the training with an AK47 (“New Edition of Inspire Magazine,” 2011). The magazine, known for its high production standards, is aimed to radicalize English-speaking Muslims, encouraging them to engage in militant activity. Inspire encourages jihadist to mount attacks where they live (Stewart, 2011; Sivek, 2013). Inspire number 11 (2013) is a special issue devoted to the prime enemy, the USA. In it you find a message to the American nation, another message to American Muslims, comment on the Boston Marathon bombings, and a column on “America’s Bitter Harvest.” The last page of this aspire-to-inspire magazine contains instructions how to communicate with the editors, with two email addresses and the public key for the Asrar al-Mujahideen (Mujahideen Secrets) program. Mujahideen Secrets is the main encryption tool of the jihadist. It was put out in January 2007 by the Global Islamic Media Fund. It provides users with five encryption algorithms, advanced encryption keys and data compression tools (Lappin, 2011, p. 32). Mujahideen Secrets 2 was released in January 2008 via an Arabic-language Website set up by an Islamic forum called al-Ekhaa (Vijayan, 2008).


The military wing of Hamas, the Ez-zed-din al Qassam Brigades, has its own Website (http://www.qassam.ps/). It provides report 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” (NEW HAMAS COMIC, 2002).

I should also mention moqawama.org, the Islamic Resistance Support Association, affiliated with the Hezbollah. Information is provided in four languages: Arabic, English, French and Spanish. This is a comprehensive, regularly updated site. It presents political declarations, public statements, transcripts of speeches given by Sheikh Nasrallah, photos, songs celebrating jihad, regional and international news, and audio and video libraries.

3.3. Networking

The Internet can help bridge the gap from the isolated potential mujahid to the global jihad (Sageman, 2004, p. 163). Connection between people may start on social networking sites such as Facebook, Twitter and Vibe (a platform similar to Twitter but is anonymous and does not require identification) and then may continue on more obscure forums. The most popular twitter accounts in April 2012 were @Hamed_Alali (28,728), @HSMPress (12,499 followers), and @alemarahweb (7,153) (Zelin, 2013, p. 13). Twitter is used for breaking news, rapid responses and to cover live violent events (Zelin, 2013, p. 16).

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 (Atwan, 2006, p. 144). Young Muslim men and women share their hopes and dreams with their virtual friends on these radical forums. Some might have joined a given forum out of a sense of alienation, of feeling alone. It is estimated that a few hundreds of jihadist forums and website exist (General Intelligence and Security Service, 2012, p. 6). 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 imagined Muslim nation (Sageman, 2008, p. 116). Among the popular jihadi forums were/are: al-Qimmah, Atahadi, al-Jihad al-Alami, al-Fajr, al-Fida al-Islam (no longer active), al-Furqan, al-Faloja (no longer active), al-Hanein, Al-Luyuth al-Islamiyyah, al-Maark, al-Malahem, al-Medad, al-Shamukh, at-Tahaddi, as-Ansar, Hanein, Ansar al-Mujahideen, and The Mujahideen Electronic Network. Some of them are very large, comprising tens of thousands of people. www.shawati.com had at one point more than 31,000 registered members. www.kuwaitchat.net had more than 11,000 registered members (ICT Monitoring Group, 2012; Zelin, 2013, pp. 8-11; Chen et al., 2008, p. 259). It is estimated that some 25,000 jihadists originating from over 100 countries constitute the hard core of Internet forums (General Intelligence and Security Service, 2012).2

3.4. Psychological Warfare

Al-Qaeda regularly publishes videos that are designed to evoke fear. During the early years of the Iraq War, videos of beheadings were posted to horrify in an effort to force out the US and UK military forces and, at the same time, to recruit followers impressed by such violence (Jafarzadeh, 2007, p. 81; Atwan, 2006, p. 143; interview with Michael Nelson, former IBM Director, Internet Technology and Strategy, Woodrow Wilson Center, Washington DC, January 31, 2008). There are thousands of jihadi videos that show attacks against enemies, hostage taking, suicide bombings, operation tactics, religious inflammatory and more calculated speeches (Lappin, 2011, pp. 45-46; Salem et al., 2008). Terrorists disseminated threats of cyber terrorism, future large scale attacks and other apocalyptic warnings that keep the world’s only superpower, the USA, in constant alert.

Violence plays a key role in the psyche of jihadists. Aaron Weisburd of Haganah (http://www.internet-haganah.com/haganah/index.html), a global intelligence network dedicated to confronting global Jihad online, established
to track down jihadi sites and to inform their ISPs that they are hosting a terrorist site, looked at the prevalence of videos of explicit violence in jihadi forums in relation to the extensive data that links exposure to violence in general, and violent media in particular, to future aggression. 5% of all discussions on jihadi forums in the study (based on a random sample of 1625 discussions) existed for the sole purpose of distributing such videos of violence, in an environment that exists explicitly to promote violence (i.e. while there may be mitigating factors that keep people exposed to violent media from killing, in jihadi forums all one finds are exacerbating factors). Also, more than half of all videos distributed on jihadi forums featured explicit violence.

3.5. Socialization and Motivation

Yahoo! has become one of al-Qaeda’s most significantly useful bases of operation. Netusers utilize the Yahoo! chat functions, e-mail, and most importantly, Yahoo! Groups. Yahoo! Groups are electronic groups (e-groups) dedicated to a specific topic. Group members can read messages, contribute to the discussion, post relevant articles and multimedia files, and share a meeting place for those with similar interests. Group members may reply at their own leisure. Lycos (http://www.lycos.co.uk/) has also been used for social networking. On Orkut, an Internet service owned by Google, jihadists used to share videos and web links, promote their cause and recruit jihadists (Hunt, 2006, p. 4A). Philip Mudd, Associate Executive Assistant Director, National Security Branch, Federal Bureau of Investigation, said that young students talk in chatrooms about jihadi issues. Many of them are Muslims. Their knowledge of Islam is limited. Those young people are emotionally-driven by images from Iraq, Afghanistan and Palestine. They become motivated and wish to retaliate. In the chatrooms, they converse about Islam, Jihad, Afghanistan, Iraq, the Israeli-Palestinian conflict. The scope of such discussions is broad (interview with Philip Mudd, Woodrow Wilson Center, March 25, 2008).

3.6. Fundraising

Some terrorist groups raise funds via the Internet by five primary methods:

- **By making appeals via e-mail or directly through their websites:** The front pages of Laskar Jihad featured details of its bank accounts, in order that donations could be sent to further its aims (Bunt, 2003, p. 104). 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 (Gunaratna, 2004, p. 140; interview with Brian Marcus, former ADL Director of Internet Monitoring, Washington, DC, April 16, 2008). On the first page of the English version of its subscription satellite television station website, manartv.com, Hezbollah used to make a direct appeal for the funding of the “sustenance of the Intifadah” with the relevant bank account information for donors to do so. Account numbers were also listed on the site of the Islamic Centre of England (ICE) (http://www.ic-el.com/en) a group associated with Iran. ICE offered courses to interested parties and from time to time made appeals for donations (e.g., Pakistan Floods Appeal). It may or may not have been clear to donors where their money was going, whether to the stated cause or to another, but because of heightened vigilance in the United Kingdom, the wording of the site was careful (Gunaratna, 2004, p. 140);
- **By 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 (Weimann, 2006, p. 54);
- **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 (Rollins and Wyler, 2010; Jacobson, 2010; Levitt, 2011; United Nations Office on Drugs and Crime, 2012). 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 (Becker, 2011);

• Through 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 (interview with Mary E. Galligan, FBI Chief Inspector, Woodrow Wilson Center, June 20, 2008). Charities are legitimate front organizations which enable to raise money from across the globe. Tamimi (2007, p. 109) claims Hamas has raised millions of dollars by charity organizations in Europe, the Middle East and the United States;

• Through fraud, gambling, or online brokering: Jean-Francois Ricard, France’s top anti-terrorist investigator, argues that many terror groups finance their activities through credit card fraud (Conway, 2005, p. 8; Guiora, 2011, pp. 111-135). Imam Samudra, who was charged with the Bali bombings, published a book while in jail urging fellow Muslims to commit credit card fraud (Swartz, 2005, p. 3B; Sipress, 2004, p. A19). 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 (“A world wide web of terror – Internet jihad,” 2007; Corera, 2008; interviews with Philip Mudd, Associate Executive Assistant Director, National Security Branch, Federal Bureau of Investigation, Woodrow Wilson Center, Washington DC, March 25, 2008, and with Brian Marcus, former ADL Director of Internet Monitoring, Washington, DC, April 16, 2008). Younes Tsouli, Waseem Mughal and Tariq Al-Daour, based in London, worked for al-Qaeda 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-Qaeda (Krebs, 2007; Jacobson, 2010, p. 358).

In the United States, al-Qaeda has received funds from numerous social charities. In the wake of September 11, 2001 terror attack, the U.S. government seized or froze the assets of several charities, among them The Benevolence International Foundation, Elehssan Society (USA: Treasury designates charity as conduit for terrorism funding, 2005), The Global Relief Foundation (US Department of the Treasury), Goodwill Charitable Organization (US acts on groups aiding Hezbolla, 2007), The Holy Land Foundation for Relief and Development (Anonymous, 2003; Holy Land Foundation Shut Down, 2001), Al Kifah Refugee Center (Profile: Al-Kifah Refugee Center), The Union of God (Jacobson, 2010, p. 356), and The Al-Haramain Foundation (Cosgrove-Mather, 2004) that allegedly used the Internet to raise money for al-Qaeda and Hamas (ADL, 2002).

3.7. Spreading Tactics: Instructions and Online Manuals

Multiple password-protected forums refer to extensive literature on explosives. There are 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 (Sageman, 2008, p. 113).

In addition to manuals and diagrams, training videos have become increasingly common among terrorist websites (Forest, 2006, p. 10).

Many of these sites post the Terrorist’s Handbook (http://www.capricorn.org/~akira/home/terror.html) and The Anarchist Cookbook (http://www.scribd.com/doc/387846/The-Anarchist-Cook-Book), two well-known manuals that offer detailed instructions of how to construct a wide range of bombs. These “classic” manuals are supplemented with al-Qaeda own how-to books, whose writing has benefited from vast experience in the battle fields of Iraq, Afghanistan and other bloody theatres. The Mujahideen Poisons Handbook, written by Abdel-Aziz in 1996 and published on the official Hamas website, details how to prepare various homemade poisons, chemical poisons, poisonous gases, and other deadly materials for use in terrorist attacks (http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDEQFjAA&url=http%3A%2F%2Fforum.xumuk.ru%2Findex.php%3Fapp%3Dcore%26module%3Dattach%26section%3Dattach%26attach_id%3D5059-%ce=E7n8UfalHHeTiALjvIGYDw&usg=AFQjCNHKM8wYGxveV6Y58ENXTrSV-1bV7w&sig2=XN2a50LcSzvQ6L4xGnE57Q&bvm=bv.50165853,d.cGE). The Mujahideen Explosives Handbook (http://www.riskintel.com/wp-content/uploads/downloads/2011/06/Mujahideen-Explosive-Book.pdf) also written by Abdel-Aziz, teaches how to prepare a laboratory, how to cut glass pipe tube, and how to handle hot substances. Interestingly, the Handbook opens by a call to scan military books and send them to the Organization for the Preparation of Mujahideen (O.P.M.) by using encrypted e-mail. The public key of the Pretty Good Privacy (PGP) encryption software was provided together with the key ID.

The so-called Encyclopedia of Jihad (http://www.washingtonpost.com/wp-dyn/content/custom/2005/08/05/CU2005080501351.html) created by al-Qaeda, offers instructions on the manufacture of weapons and explosives, first aid, analyzing intelligence information, American military training, establishing and operating an underground network, and detailed guidelines on carrying out violent attacks (Malashenko, Bowers and Ciobanu, 2001).

The Al-Qaeda Manual is comprised of eighteen lessons. The Manual equips the modern Muslim warrior with the necessary information to carry out duties without being caught. Thus, for instance, lesson three concerns counterfeit currency and forged documents. Lesson four is about hiding places. Lesson five is concerned with communication and transportation. Lesson seven discusses weapons while lesson eight is about members’ safety. Lessons eleven and twelve are about espionage while lesson eighteen is about prisons and detention centers.

The Encyclopedia of the Afghan Jihad (http://www.unl.edu/eskridge/encyclopedia.html; http://emp.byui.edu/ANDERSONR/ite/Book%20_of_Mormon/08_helaman/helaman01/helaman01_08terrorism.htm) is a detailed Jihad manual which explains how to make and use explosives and firearms, and how to plan and carry out assassinations and terror attacks. The manual urges that plans should be laid out to hit buildings such as skyscrapers, ports, airports, nuclear plants and football stadiums, suggesting attacking large congregations at Christmas (Smith and Destiny, 2008; Akdeniz, 2009, p. 12).

Jihadists also benefit from freely available manuals that exist on the Net. For instance, Bacteriological Warfare: A Major Threat to North America (http://www.101rl.com/survivalfiles/files/chem/bacteriological%20warfare.pdf) was written by microbiologist Larry Wayne
Harris (1995). It is aimed to warn against the use of certain bacteria by terrorists. At the same time, it provides valuable data that might be exploited by terrorists. Harris ends his book (1995, p. 130) by saying that the public wants biological civil defense. “The public does not know that the government has failed to provide the Biological civil defense program which will preserve our society in the event of Terrorist Germ Warfare attacks.” However, the failure may be attributed in part to this very detailed book.

3.8. Recruitment

There are numerous cases of normal, often non-religious citizens becoming radicalized by jihadist websites, leaving them vulnerable to terrorist recruitment (Hoffman, 2010; Harman, 2010; Hewitt, 2008, p. 40). 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.

Online recruiting has increased exponentially due to two converging developments: On the one hand, the increased intelligence work of security forces to scrutinize Muslim community centers and mosques; on the other hand, the increased popularity of Facebook, MySpace, Orkut, Friendster, YouTube and other social networking sites which attract interested jihadists who play a critical role in identifying potential radicals and alert about suspected others. There are hundreds of pages dedicated to Osama Bin Laden, Abdullah Azzam and other heroes of the mujahideen (Atwan, 2012, p. 240; Witte, Markon and Hussain, 2009). Using the Internet, terrorist organizations can seek potential jihadists by using advanced technologies to showcase their ideas and achievements, and to learn about interested users. Those who deemed most interested in the organization’s cause, or most likely to be useful in carrying out its work, can be contacted. Electronic bulletin boards and issue-specific chatrooms are used to reach out and draw in potential recruits (Combs, 2006, p. 142). Videos are intended to impress people associated with radical Websites to travel to militant training camps in Pakistan.

Terrorist groups in Iraq, Afghanistan, Pakistan, Somalia, Yemen (al Qaeda cleric Anwar al-Awlaki) (Obituary: Anwar al-Awlaki, 2011) and other parts of the Middle East have used the Internet to recruit American and European Muslims. One of the most significant postings was made by al-Zarqawi in 2004 to announce his allegiance to bin Laden and to al-Qaeda (Figure 2). As this news flashed around the globe it became an open invitation to all al-Qaeda would-be jihadis to flock to Iraq, which many did (Atwan, 2006, p. 142; Venzke and Ibrahim, 2003). In June 2004, the magazine Insight Online obtained a recruitment appeal seeking Iranians who would commit suicide in deadly attacks on U.S. and coalition forces in Iraq, on Israel, and on American citizens around the world. Some 10,000 people were said to register to carry out martyrdom operations (Forest, 2006, pp. 57-58).

3.9. Planning of Activities and Coordination

Terrorists use the Internet not only to learn how to build bombs but also to plan and coordinate specific attacks. 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.

Hamas supporters in the Middle East use chatrooms to plan and coordinate operations, exchanging e-mails across Gaza, the West Bank, Lebanon, and Israel (Combs, 2006, p. 143). Al-Qaeda became a web-directed guerrilla network. It planned attacks years in advance, inserted sleeper cells, and did reconnaissance.
They took the long view, believing that their struggle would take decades, perhaps generations (Clarke, 2004, p. 227). Al-Qaeda used the Internet to orchestrate all its major attacks since the two embassy bombings in Nairobi and Dar-es-Salaam in 1998. The Internet has become a key element in al-Qaeda training, planning and logistics, and cyberspace a legitimate field of battle (Atwan, 2006, pp. 122-131; National Security Program, 2012).

Al-Qaeda 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-Qaeda terrorists learned the methods used by the U.S. to combat terrorism; they studied the American soft spots and targets. Al-Qaeda 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-Qaeda 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 (interview with Mary E. Galligan, FBI Chief Inspector, Woodrow Wilson Center, June 20, 2008). 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 U.S. 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 (Bobbitt, 2008, p. 308; Firestone and Canedy, 2011, p. A3). Thousands of code-word and encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested al-Qaeda senior terrorist Abu Zubaydah. The first messages found on Zubaydah’s computer were dated May 2001, and the last were sent on September 9, 2001, two days before the attacks that dramatically affected world affairs. The frequency of the messages was highest in August 2001 (Weimann, 2006a, pp. 126-127).

4. COMBATING TERROR

Combating terrorism is an enormous task. It demands resources and capabilities that most of us -- normal citizens -- do not have. The prime responsibilities lie with the ISPs, with nations of the free world, and with the international community at large. As terrorism is a global phenomenon, it is necessary to fight against it globally via cross-country diligent cooperation.
Terrorist are careful in their use of the Internet. Training websites are frequently moved from one web server to another. Coded messages are posted to chatrooms and discussion forums, through which new websites addresses for terrorist information are made available. Sensitive information is encrypted with freely available technology. Participation in encoded forums is by invitation only. New participants are inspected closely before trusted to gain access. Closed forums also receive material from al-Qaeda Central for distribution to the greater audience (Sageman, 2008, p. 119).

4.1. ISP Responsibility

Like in any other forum and industry, there is a need to assure a certain security level on the Internet. American Internet Service Providers hosted terrorist sites and helped the cause of jihad. Some did it knowingly while others did it inadvertently. Thus, for instance, InfoCom Corporation in Texas hosted websites for numerous clients in the Middle East. It served more than five hundred Saudi Internet sites and notable Palestinian Hamas organizations, including the Islamic Association for Palestine and the Holy Land Foundation for Relief and Development. InfoCom was founded by Mousa Abu Marzook, one of the leaders of Hamas. InfoCom also served to launder money. Large amounts of money came from Saudi Arabia and the Gulf states to sponsor Hamas activities (Anonymous, 2003, pp. 262-263; Whitaker, 2001; Investigative Project on Terrorism).

While InfoCom directors knew exactly what they were doing, Fortress ITX unwittingly hosted a jihadi site that urged attacks against American and Israeli targets. Among the web pages were “The Art of Kidnapping,” “Military Instructions to the Mujahideen,” and “War Inside the Cities.” The informative site was shut down after Fortress learnt about the content from a reporter (Lichtblau, 2004). Undoubtedly, not playing into the hands of terrorists requires over-viewing and proactive steps. ISPs are reluctant to monitor their servers for economic reasons. American ISPs do not see monitoring as part of their service. They often claim they do not wish to compromise their customers’ First Amendment rights (Cohen-Almagor, 2010).

If an ISP hosts a terrorist site, the owner can be charged with conspiracy and aiding and abetting terrorism. But unfortunately, still many of the terrorist websites are hosted by servers in the western world. Intermediaries, such as ISPs and Web-Hosting Services (WHSs), can play a useful role in offering the public a regulating or authenticating service. That is, ISPs and WHSs can market their Internet access software by promising to include certain kinds and quality of content and exclude others. ISPs and WHSs would compete with each other on the basis of the cluster of options they offer as well as over their software-based filtering systems (National Research Council, 2001, p. 228).

Codes of conduct should be adopted to ensure that Internet content and service providers act in accord with the law and with principles of social responsibility. These codes should meet community concerns and industry needs, operating as an accountability system that guarantees a high level of credibility and quality (Cohen-Almagor, 2006). To be effective, these codes of conduct should be the product of and be enforced by self-regulatory agencies. Because of the transnational nature of Internet communications, coordinated activity among such agencies in different jurisdictions needs to be an essential element of self-regulation. And there should be widespread use of rating and filtering technology. To this end, content providers should be mobilized to label their content voluntarily, and filters must be made available to empower Netusers to make effective choices about information received. The effectiveness of the self-regulatory mechanisms should be measured in order to determine what national and transnational measures—if any—are necessary to compensate for their deficiencies (Waltermann and Machill, 2000, p. 37).

The use of hotlines can establish new routes of communication between Netusers, in particular, parents, media-industry initiatives, and law enforcement authorities. A hotline enables
users to respond to illegal Internet content by drawing attention to where it is to be found. The hotline receives the report and, if necessary, sets in motion a process of response. The response includes processing the report, providing the Netuser with feedback and a decision about whether to forward the report to law enforcement or a self-regulatory authority (Waltermann and Machill, 2000, p. 17). Netusers who might not wish to alert the police directly should be able to contact a cyber tip line and evoke attention to violent threats and signals.

### 4.2. State Action

One of the prime responsibilities a state has to its citizens is to provide them with the ability to lead their lives in peace, free of existential threats and violence. Caution and reasonableness are prerequisites to address violent, anti-social challenges sensibly and cautiously, without evoking unnecessary panic. While realizing that some boundaries need to be introduced to liberty and tolerance in order to maintain a responsible Internet, we should be careful not to exaggerate the challenges. The course of action needs to be measured, without instilling chilling effects that might silence Netusers and organizations. Evoking fear only plays into the hands of terrorists.

There is a lot countries can do in terms of mapping terrorist groups, tracking the various connections between terrorist organizations as well as the connections between terrorists and criminals. The challenge is to explore the Deep Web. Also known as the Deep Net, and sometimes as the Dark Net, the Deep Web refers to the alternate, clandestine side of the Internet which is used by criminals, terrorists, and extremist groups to cooperate, spread their ideas and promote their anti-social, criminal and violent causes. It contains data crafted deliberately to lie beyond the reach of search engines. According to a 2009 Deep Web research, there are 1 trillion pages located on the World Wide Web in various files and formats that search engines either cannot find or have difficulty accessing (Zillman, 2009).

After September 11, 2001, the United States has been dedicating large resources to combat local and global terrorism. US law enforcement agencies had set up websites that resemble Jihadi sites to lure terrorists and extremists. These honey-pots enable tracking visitors by their electronic trails (Frantz, Meyer and Schmitt, 2004, p. A1). In an interview, Philip Mudd explained the mode of operation to counter terror on the Net. He said that the general approach is to look at people. The FBI receives information about individuals who might risk security and then follows their actions, including on the Internet. The FBI examines the sites they surf. Typically the FBI does not monitor the Net: “We go after people who we suspect, not websites. If the bad people go to sites, we follow them” (interviews with Philip Mudd and John Morris, The Center for Democracy and Technology, Washington DC, March 25, 2008 and February 7, 2008). Mudd maintained that Internet providers should have integrity teams, instructing providers to take off dangerous content. He wanted to put the onus of responsibility on them. The FBI official further stressed the need to better understand the Internet’s social networking sites, notably Facebook. What are the implications of these tools on terrorism? Considerable efforts are invested to track down terror-related Internet forums. Once tracked, the FBI is reluctant to shut them down (interview with Philip Mudd, Washington DC (March 25, 2008; discussion with senior FBI officials, Washington DC, March 26, 2008). It prefers to keep an open eye on them.

FBI officials are proud in their ability to provide security to American citizens after the shocking tragedy of September 11. However, more need to be done in harvesting and collecting information about jihadi websites, blogs, chatrooms and other forms of Internet communication in order to fully understand terror campaigns. Government agencies may gain valuable information about terrorist and criminal activities by monitoring designated
sites. Developed mechanisms to scrutinize large parts of the Internet susceptible to criminal activity are available (Evans, 2004, p. 498).

The American government relies on the work of private individuals and organizations that monitor jihadi chatrooms. Among them are the Terrorism Research Center (http://trc.uark.edu/), The Search for International Terrorist Entities (SITE) Intelligence Group (http://news.siteintelgroup.com), and the Northeast Intelligence Network (http://homelandsecurityus.com/). Notable individuals who took upon themselves to monitor terrorism are Aaron Weisburd of Haganah, and Evan Kohlmann who describes himself as a private sector international terrorism consultant (https://flashpoint-intel.com/about.php). The bigger groups employ Arabic linguists, a scarce and vital resource that can help win lucrative contracts (Labi, 2006). Knowledge of Arabic (the most prominent language in jihadi forums), Dari, Farsi, Urdu, Pashto, among other languages, is vital in the fight against modern forms of terrorism. Also vital is the understanding of the specific tribal-cultural codes of the jihadists. Knowledge of language is essential but it might not be sufficient for exhaustive comprehension of communication.

In the name of freedom of expression, freedom of information and the public’s right to know, USA – the land of the First Amendment – made highly sensitive information freely available on the Internet. The information included details about potential targets, e.g., nuclear power plants, gas and oil stores, water pumps and supply, toxic-release inventory, list of key factories, emergency services, medical computer systems, powerful generators, wastewater treatment plants, disaster control services, dams, bridges, and detailed maps of the nation’s infrastructure (McKinley, 2002, p. B1). Only after September 11, 2001, US ministries and agencies realized that such sensitive information in the wrong hands might be very risky, undermining State security. Only then, in fighting terrorist data mining, government and non-governmental organizations removed sensitive data from the Internet. The Agency of Toxic Substances, the Emergency Management Office, the Federal Aviation Administration (FAA), National Aeronautics and Space Administration (NASA) and the Department of Transport are among those agencies that removed potentially damaging information about the US social and economic infrastructure from the Internet.

The fight against terrorism is not merely an American concern. While the US took upon itself a leading role in this international and most sophisticated struggle, other democracies also invest in counter-terrorism. With the United States, the United Kingdom, Canada, Australia and New Zealand are also using the Echelon program to intercept Internet transmissions. The UK Terrorism Acts of 2000 and 2006 contain provisions criminalizing the encouragement of terrorism (Part 1, 1) and the dissemination of terrorist publications (Part 1, 2). The Acts prohibit sharing information that could be useful to terrorists, videos of violence which contain praise for the attackers (Part 1, 20), chat forums with postings inciting people to commit terrorist acts, and instructions as to how to make weapons, poisons and bombs. The Acts also include notice and take down provisions if the encouragement or dissemination takes place over the Internet (Part 1, 3) (Reporting extremism and terrorism online). The Acts provide a method by which webmasters could be made aware of terrorist content, thus ensuring that they could not claim not to have known about it if they were subsequently prosecuted (Akdeniz, 2008, p. 239).

4.3. International Cooperation

As aforesaid, terrorism has global networks and therefore tackling it requires international cooperation. Follow the money is a good advice for the combat of terrorism. The ability to stop the flow of funds via the Internet to terrorist organizations is difficult and time-consuming (Combs, 2006, pp. 144-145). 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 cyber worlds, multilateral bod-
ies such as the Financial Action Task Force (FATF) (http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html), 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 terrorist masquerading as charities, and establishing international standards to combat such abuse. Another step in the right direction is the 1999 UN International Convention for the Suppression of the Financing of Terrorism.

On September 8, 2006, the United Nations adopted a Global Counter-Terrorism 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. This was the first time that all Member States agreed to a common strategic approach to combat terrorism, sending a clear message that terrorism is unacceptable in any form and also resolving to take practical steps to fight against it. Those practical steps range from strengthening state capacity to better coordinating UN counter-terrorism activities (UN Action to Counter Terrorism).

In 2007, European Union states began to share monitoring of militant websites, including sites linked to al-Qaeda. Keeping track of jihadi sites requires vigilance as statements and videos by individuals and groups may appear only for a short period of time. The Internet increases in volume each and every day, and its security is difficult to maintain. I have mentioned the links between terrorism and organized crime. Narcterrorism, the confluence between drugs and terrorism that simultaneously advances distinct and mutual interests of terrorists and criminals is a real concern. The cooperation between unlawful elements is designed to facilitate one another and is instrumental in devising ways to overcome national and international efforts to stifle their illegal activities.

In July 2007, the European Commission announced plans to frustrate terrorism by suppressing online guides on bomb-making. European ISPs would face charges if they failed to block websites with bomb-making instructions (Page, 2007). The EU police agency, Europol, has built an information portal to allow exchange of information on militant websites monitoring. The portal includes a list of links of monitored websites, statements by terrorists, and information designed to fight down terrorism (Melander, 2007).

5. CONCLUSION

Terrorists are trained to be technologically savvy and to attack, disrupt, damage and perhaps even destroy technology infrastructures and computer-based economic activities. The Internet has become a major vehicle for promoting their ends. The structure of the Internet has facilitated the global Islamist terrorism. It has evolved through the search and exploration of new safe methods of interaction by thousands of terrorist sympathizers. Many modern terrorist groups share the pattern of the loosely knit network; decentralization, segmentation, and delegation of authority. These features make computer-mediated communication an ideal tool of coordination, information exchange, training, and recruitment (Weimann, 2006, p. 116). The Internet has grown to be a key element in al-Qaeda training, planning and logistics.

Many terrorists begin their journey to violent jihad on the Internet (Jenkins, 2010, p. 4). Radical forums create virtual communities, connect between people, provide rich information on timely topics, reinforce beliefs and normalise violent behaviour. Thousands of websites and bulletin boards offer videos, images, statements, and speeches that demonstrate the Internet’s centrality to global terrorism. Great reverence is paid to the views of the militant leadership. Anti-western videos showing non-Muslims humiliating Muslims populate the Internet in order to win the hearts and minds of potential followers. The Internet has taken on huge importance for militant groups, enabling them to share know-how (e.g. bombmaking,
suicide bombing, guerrilla operations) and spread propaganda to a mass audience, and to plan operations.

The Internet is the single most important factor in transforming largely local jihadi concerns and activities into the global network that characterizes al-Qaeda today (Atwan, 2012, pp. 235-245). The Internet is ubiquitous, interactive, fast and decentralized. The ease of access to the Internet, its low cost and speed, its chaotic structure (or lack of structure), the anonymity which individuals and groups may enjoy, and the international character of the Net furnish all kinds of individuals and organizations an easy and effective arena for their partisan interests. Law-enforcement agencies throughout the world can learn from each other and cooperate in the fighting against illicit and anti-social activities on the Net. Indeed, there are many similarities between counter-online terrorism activities, counter-online child-pornography activities, and counter-online racism activities (Cohen-Almagor, 2011, 2013). Further research is required on the differences and similarities of utilizing the Internet for different criminal and anti-social activities and how to combat them. This research has many practical implications thus it should involve collaborative efforts between academic researchers and law-enforcement agencies.

As years passed, there is more awareness of the threats and of the needs in order to provide social security. Ignorance, whether circumstantial or normative, cannot serve as an excuse. The international community is expected to take the necessary responsible measures to promote security online. With the right cooperation, the international community has the capabilities to address the formidable challenges and provide appropriate answers. Indeed, to have effective results in fighting down terrorism, cooperation is vital. Failure to do so is inexcusable. Without responsible cooperation, Net abusers will prevail and our children suffer. Nations and responsible Net-citizens are obliged to ensure that our future generations will be able to develop their autonomy, their individuality and their capabilities in a secure environment, both offline and online.

**REFERENCES**


FATF. http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html


Harman, J. (2010). Internet terror recruitment and tradecraft: How can we address an evolving tool while protecting free speech?. Statement before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment (Washington, May 26).


Hoffman, B. (2010). Internet terror recruitment and tradecraft: How can we address an evolving tool while protecting free speech?. Statement before the House Committee on Homeland Security (Washington, May 26).


*Mujahideen Poisons Handbook*: 1, http://www. google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDEQFjAA&url=http%3A%2F%2Fforum.xumuk.ru%2Findex.php%3Fapp%3Dcore%26module%3Dattach%26section%3Dattach%26attach_id%3D5059&ei=E7n8UfalHIeTiALjvIGYDw&usg=AFQjCNHKM8wvYGvxeV6Y58ENXTrSV-1bV7w&sig2=3X2a50Le5vQX6L4xGnE57Q&bvm=bv.50165853,d.cGE


Northeast Intelligence Network. http://homeland-securityus.com/


Stewart, S. (2011). How to tell if your neighbor is a bombmaker. Straturf (April 7).

Swartz, J. (2005). Terrorists’ use of Internet spreads. USA Today (February 21), 3B.


Terrorist’s Handbook http://www.capricorn.org/~akira/home/terror.html


Tor: Overview, Tor, torproject.org/about/overview.html.en

TRC. http://trc.uark.edu/


Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
USA. Treasury designates charity as conduit for terrorism funding (May 5, 2005), http://www.bankingsurveillance.com/aml_cft/USA-Treasury-designates-charity-as-conduit-for-terrorism-funding


What is a Tor Relay? Electronic Frontier Foundation, https://www.eff.org/torchallenge/what-is-tor


ENDNOTES

1 For discussion on the complicated task of defining terrorism, see Schmid (2011, pp. 39-98) and Martin (2011, pp. 2-25).

2 Zelin (2013, p. 2) estimates the number of active jihadi forums in 2012 to be three to five.

3 Communication with Aaron Weisburd (December 22, 2008).

4 For a fascinating account of the connection between terrorism and charity organizations in the USA, see Anonymous (2003). See also Zaitz (2003, p. B1).

5 The BIF, based in Illinois, was founded in the 1980s by Saudi sheikh Adil Abdul Galil Batargy. BIF described itself as a humanitarian organization dedicated to helping those afflicted by wars. According to the FBI, the BIF raised millions of dollars for bin Laden. It also reportedly sent $600,000 to Chechen extremists trained by al-Qaeda. See Anonymous, 2003, pp. 192-193, 209.

6 PGP is a widely available software package permitting Netusers to use encryption when exchanging messages.