Virtual Terrorism:
How Modern Terrorists Use the Internet

> Conflicts on the ground are echoed, as one can imagine, in cyberspace… Cyberspace offers even more fertile territory for sabotage, misinformation, and what in the cliched formulation is termed the war over minds.
>
> Vinay Lal
> (Terror and Its Networks: Disappearing Trails in Cyberspace)

Abstract

The nature of the Internet - the ease of access, the chaotic structure, the anonymity, the "liberal spirit", and the international character - all furnish terrorist organizations with a new, easy and effective arena for action. However, counter-terrorism measures, especially those introduced after the September 11 attacks in New York and Washington, raise serious concerns about restricting free expression and free flow of information. This paper focuses on this new battle, examining both the uses of the Internet by modern terrorist organizations and the costs of the attempts to prevent them. How do modern terrorists use the Internet and for what purposes? How can governments respond to this new challenge? This paper reports some of the findings of a seven-year monitoring of about 5,000 terrorist websites

using a qualitative content analysis to learn about rhetorical structures, symbols, persuasive appeals, target audiences, interactivity and communication tactics. Finally, the study will examine various implications for policy making regarding terrorism and the Internet, especially with regard to its accessibility, boundaries on freedom of speech and usability for the spread of hate and violence.

Introduction

The story of the presence of terrorist groups in cyberspace has barely begun to be told. In 1998, less than half of the 30 organizations designated as Foreign Terrorist Organizations maintained websites[i]; by the end of 1999, nearly all these 30 terrorist groups had established their presence on the Net. Today, all active terrorist groups have established at least one form of presence on the Internet. Our scan of the Internet in 2004-5 revealed thousands of websites, online forums and chat rooms serving terrorists and their supporters (Weimann, 2004). Paradoxically, the very decentralized network of computer-mediated communication that U.S. security services created out of fear of the Soviet Union now serves the interests of the greatest foe of the world's security services since the end of the Cold War: international terror. The nature of the network – its international character and chaotic structure, the simple access and the anonymity it offers – all furnish terrorist organizations with an ideal arena for action. The same advantages the Internet and advanced communication technology bring to the general public and to business -- speed, easy access and global linkage -- are helping international terrorist groups organize their deadly and disruptive activities.

The same advantages the Internet and advanced communication technology bring to the general public and to business -- speed, easy access and global linkage -- are helping international terrorist groups organize their deadly and disruptive activities. "The Internet and e-mail provide the perfect vehicles for these groups to communicate with each other, to spread their message, to raise money and to launch cyberattacks," argued Defense director of intelligence for special projects Ben Venzke. Paradoxically, the very decentralized structure that the American security services created out of fear of a Soviet nuclear attack now serves the interests of the greatest foe of the West's security services since the end of the Cold War, namely international terror. The nature of the network, its international character and chaotic structure, the simple access, the anonymity – all furnish terrorist organizations with an ideal arena for action.

It started in the early 1970s, during the heat of the cold war, when the U.S. Department of Defense was concerned about the vulnerability of its computer network to

nuclear attack. The alternative idea was decentralize the whole system by creating an interconnected web of computer networks. The net was designed so that every computer could talk to every other computer. Information was bundled in a packet, called an *Internet Protocol Packet*, which contained the destination address of the target computer. The system that the Pentagon eventually developed was called ARPANET. At about the same time, companies developed software that allowed computers to be linked to local networks (LANs) that also contained the Internet Protocol programs. The users of this early network were primarily scientists, academics and computer experts. In the late 1980s, however, the National Science Foundation, whose own network was already connected to the net, created five centers at U.S. universities. This was the birth of the Internet. Today, when students, scientists, government officials, and in fact everyone can have access to the information superhighways, to worldwide database and to the cyberspace network, the number of users, the amount of information exchanges and the time spent surfing in the cyberspace have increased tremendously. In the mid 1990's, the Internet connected more than 18,000 networks with the number increasing daily. Hooked into those networks were about 3.2 million host computers (experts estimate that about 1000 host computers are added to the net every day) and maybe 50-60 million users spread across all seven continents. The estimated number of users in the early years of the 21st century is over a billion.

When the Internet first appeared, it was hailed as an integrator of cultures and a medium for businesses, consumers, and governments to communicate with one another. It appeared to offer unparalleled opportunities for the creation of a "global village." The potential of the Internet for political purposes has fascinated many. Utopian visions of a 'virtual state' in which citizens hold daily common discussions, communicate needs and demands to their representatives, and vote by various referenda (all using computer mediated communication) have been raised by thinkers and researchers. Today the Internet still offers that promise, but it also has proven in some respects to be a digital menace. Its use by al Qaida is only one example. It also has provided a virtual battlefield for peacetime hostilities between Taiwan and China, Israel and Palestine, Pakistan and India, and China and the United States (during both the war over Kosovo and in the aftermath of the collision between the US Navy aircraft and a Chinese Mig). In times of actual conflict, the Internet was used as a virtual battleground between NATO's coalition

forces and elements of the Serbian population. These real tensions from a virtual interface involved not only nation-states but also non-state individuals and groups either aligned with one side or the other, or acting independently.

With the enormous growth in the size and use of the network, it became clear that the "utopian vision" of the Internet and its promises were challenged by the spread of pornographic and violent contents on the web and the use of the Internet by radical terrorist organizations of various kinds. Anarchists, nationalists, separatists, revolutionaries, Neo-Marxists, and fascists – were using the network to distribute their propaganda, to communicate with their supporters, to create public awareness and sympathy, and even to execute operations. The story of cyberspace presence of terrorist groups has barely begun to be told. In 1998, nearly half of the 30 organizations designated as Foreign Terrorist Organizations under the Antiterrorism and Effective Death Penalty Act of 1996 [AEDPA] maintained websites; by the end of 1999, nearly all terrorist groups had established their presence on the net. These websites, whatever other language versions they might be available in, are invariably in English and pose complex and hitherto unexplored questions about the constituencies that find cyberspace hospitable for the fulfillment of their political goals.

Terrorism and Communication

The emergence of media-oriented terrorism led several communication and terrorism scholars to re-conceptualize modern terrorism within the framework of symbolic communication theory (Jenkins 1975; Weimann, 1986; Weimann & Winn, 1994). Karber has pointed out that “the terrorist’s message of violence necessitates a victim, whether personal or institutional, but the target or intended recipient of the communication may not be the victim" (Karber, 1971, 529). Dowling suggested applying the concept of "rhetoric genre" to modern terrorism, arguing that "terrorists engage in recurrent rhetorical forms that force the media to provide the access without which terrorism could not fulfill its objectives" (1986, 14) while Weimann and Winn adopted the theater of terror metaphor to examine modern terrorism as an attempt to communicate messages through the use of orchestrated violence (Weimann & Winn, 1994). The growing use and manipulation of modern communications by terrorist organizations led

governments and several media organizations to consider certain steps in response. These included limiting terrorists' access to the conventional mass media, reducing and censoring news coverage of terrorist acts and their perpetrators, and minimizing the terrorists' capacity for manipulating the media (Weimann, 1999). However, the new media technologies allow terrorist organizations to transmit messages more easily and freely than through other means of communication. The network of computer-mediated communication (CMC) is ideal for terrorists-as-communicators: it is decentralized, it cannot be subjected to control or restriction, it is not censored, and it allows access to anyone who wants it.

Terrorism and the Internet are related in several ways. First, the Internet has become a forum for terrorist groups and individual terrorists both to spread their messages of hate and violence and to communicate with one another and with sympathizers. Secondly, individuals and groups have tried to attack computer networks, including those on the Internet, what has become known as cyberterrorism or cyberwarfare. At this point, terrorists are using the Internet for propaganda and communication more than they are attacking it. Former chief of operations at the FBI Buck Revell told *U.S. News and World Report* that "As long as they don't specifically engage in criminal acts, they can do anything they want to aid and abet their activities. This is a safe haven for them."

The use of the Internet by modern terrorists is well-related to the conceptualization of terrorism as a psychological warfare. Cyber-fear, argues Thomas (2003), is generated by the fact that what a computer attack *could* do (bring down airliners, ruin critical infrastructure, destroy the stock market, reveal State secrets, etc.) is too often associated with what *will* happen. It is clear that the Internet empowers small groups and makes them appear much more capable than they might actually be, even turning bluster into a type of virtual fear. The net allows terrorists to amplify the consequences of their activities with follow-on messages and threats directly to the population at large, even though the terrorist group may be totally impotent. In effect, the Internet allows a person or group to appear to be larger or more important or threatening than they really are. The Internet can be used to spread disinformation, frightening personal messages, or horrific images of recent activities (one is reminded of the use of the net to replay the murder of the Jewish-American reporter Daniel Pearl by his Pakistani captors).

Given the growth of Internet research in recent years, it is rather surprising that previous research has overlooked the online activity of terrorist organizations. Who are the terrorist movements that use the Internet? What is the rhetoric of the terror sites on the Internet? Who are the target audiences addressed by the terrorists through the network? Do the organizations use the Internet to mobilize audiences for active operations? Current research leaves these questions almost unanswered. This article focuses on the use of the Internet by modern terrorist organizations and attempts to describe the uses terrorist organizations make of this new communication technology and to examine various implications for policy making regarding terrorism and the Internet and especially with regard to its accessibility, boundaries on freedom of speech and usability for the spread of hate and violence. Thus, we examine the cyberspace as a new arena for international conflicts, looking how terrorists use it, how counter-terrorist agencies fight back, examining the policy implications and the trade-offs in terms of

To fully understand the complexity of this new mode of conflict, its character, implications and potential consequences, one must distinguish among three levels of analysis. These are (a) The communicative use of the Internet by terrorism; and (c) Fighting back? Responses to terrorism on the Internet.

The Communicative use of the Internet by terrorism

One of the enduring axioms of terrorism is that it is designed to generate publicity and attract attention to the terrorists and their cause. How do terrorist groups use the Internet to advance the organization's political and ideological agenda? We know that terrorist organizations are increasingly resorting to the Internet to disseminate their views to a wider public, coming to the realization that establishing their presence in cyberspace is nearly just as critical to their long-term success as any military triumph or act of sabotage. Terrorist groups themselves can maintain webpages to "advertise" their ideology, disseminate propaganda and recruit supporters. It is the first time that they can easily reach the public directly and make their existence known in an international scale.

In the "conventional media", if some report was offensive to a government, the content of the report could be censored or filtered. However, Governments cannot control the Internet to the same degree they could control newspapers, radio and TV. The web

allows an uncensored and unfiltered version of events to be broadcast worldwide. Chat rooms, websites, and bulletin boards are largely uncontrolled, with few filters in place. This climate, argues Thomas (2003), is perfect for a radical group to explain its actions or to offset both internal and international condemnation, especially when using specific servers. The Internet can target fence-sitters as well as true believers with different messages, oriented to the target audience. Thus, for example, in the aftermath of the 9/11 attacks, al Qaeda operatives used the Internet to fight for the hearts and minds of the Islamic faithful worldwide. Several internationally recognized and respected Muslims who questioned the attacks were described as hypocrites by al Qaeda. Al Qaeda ran two websites, alneda.com and drasat.com, to discuss the legality of the attacks on 9/11. Al Qaeda stated that Islam shares no fundamental values with the West and that Muslims are committed to spread Islam by the sword. As a result of such commentary, several Muslim critics of al Qaeda's policies withdrew their prior condemnation.

Two earlier studies reveal the growing attraction of the Internet to modern terrorists. Tsfati and Weimann applied a systematic content analysis to a sample of terrorist sites, and repeated this analysis after 3 years (Tsfati and Weimann, 1999, 2002). They used the American State Department's list of terrorist organizations (U.S. State Department, 1996; US State Department, 2000), which meets the accepted definition of terror (as elaborated by Schmid & Jongman, 1988) and located the terror sites using the names of hundreds of organizations in the sampling base. The 1998 search was limited to English websites, while the 2002 search included sites in English and Arabic. All the organizations active in 1998 were also online in 2002 but additional terrorist sites were found in the later study. While the 1998 study revealed 12 terrorist sites the last monitoring of the Net in 2005 found 4,750 websites serving terrorist organizations and their supporters (Weimann, 2005).

Who are the terrorist organizations in the web? All modern terrorists are using the Net, and most of them in more than one forms of presence and in several languages. The list includes the Hamas (the Islamic Resistance Movement), the Lebanese Hizbollah (Party of God), the Egyptian Al-Gama'a al Islamiyya (Islamic Group, IG), the Popular Front for the Liberation of Palestine (PLFP), the Palestinian Islamic Jihad, the Peruvian Tupak-Amaru (MRTA) and 'The Shining Path' (Sendero Luminoso), the Kahane Lives

movement, the Basque ETA movement, the Irish Republican Army (IRA), the Japanese Supreme Truth (Aum Shinrikyo), the Colombian National Liberation Army (ELN-Colombia), the Liberation Tigers of Tamil Eelam (LTTE), the Armed Revolutionary Forces of Colombia (FARC), the Popular Democratic Liberation Front Party in Turkey (DHKP/C), the Kurdish Workers' Party (PKK), the Zapatista National Liberation Army (ELNZ), the Japanese Red Army (JRA), and the Islamic Movement of Uzbekistan (IMU), the People's Mujahedin of Iran (PMOI - Mujahedin-e Khalq) and others. All these organizations not only pursue the peaceful act of establishing Internet sites, but also engage in actual violence (some of them with a long record that includes killings, kidnapping, assaults, and bombings).

What is the content of terrorist sites? They usually include information about the history of the organization and biographies of its leaders, founders, heroes, commanders or revered personalities, information on the political and ideological aims of the organization, and up-to-date news. Most of the sites give a detailed historical review of the social and political background, a selective description of the organization's notable activities in the past, and its aims. National organizations (separatist or territorial) generally display maps of the areas in dispute: the Hamas site shows a map of Palestine; the Colombian site shows a map of Colombia; the Tamil site presents a map of Sri Lanka.

Almost all the terror sites detail their goals in one way or another. The most common presentation of aims is through a direct criticism of their enemies or rivals. Thus, the terrorist sites do not concentrate only on information concerning their organizations; direct attack of the enemy is the most common strategy of the Internet terrorists. By contrast, almost all sites avoid presenting and detailing their violent activities. Although the organizations behind these sites have a record of bloodshed, they hardly ever record these activities on their sites. The exceptions are Hizbollah and Hamas whose sites show updated statistical reports of its actions ('daily operations'), the number of dead 'martyrs,' along with the number of 'Israeli enemies' and 'collaborators' killed. However, this detailed depiction of violent action is unusual.

While avoiding the violent aspects of their activities, the Internet terrorists, regardless of their nature, motives or location, usually stress two issues: freedom of expression and political prisoners. The terrorists appear to aim at Western audiences who are sensitive to the norms of freedom of expression and emphasize the issues that

provoke sympathy in democratic societies. Restricted expression by political movements is contrary to the fundamental and sacred principles of democracy. This tactic works particularly well on the stage of the Internet, the symbol of absolutely free communication. Another theme is that of political detentions. The organizations' websites emphasize the anti-democratic measures employed against them. In so doing, they attempt to malign the authorities, appealing both to their supporters ('constituents') as well as to more remote audiences of 'bystanders.' Even among the community of their 'enemies,' namely the public that is naturally hostile to the organization, the terrorists try, by emphasizing the threats to democracy, to create feelings of uneasiness and shame.

A common element on the terror sites is the organization's communiqués and the speeches and writings of its leaders, founders, and ideologists. The sites often present a word-for-word series of official statements by the organizations, which the visitor can browse through, along with selected announcements arranged by date. They tend to recycle materials distributed in the past through the mass media and other communication means. Some terrorist sites house a veritable online gift shop through which visitors can order and purchase books, video and audiocassettes, stickers, printed shirts, and pins with the organization's badges.

What is the rhetoric of terrorist sites? Tsfati and Weimann found four rhetorical structures frequently used on the terrorist sites, all used to justify the use of violence. The first one is the "no choice" motive. Violence is presented as a necessity foisted upon the weak as the only means with which to deal with an oppressive enemy. A second rhetorical structure related to the legitimacy of the use of violence is the demonizing and de-legitimization of the enemy. The members of the movement or organization are presented as freedom fighters, forced against their will to use violence because a ruthless enemy is crushing the rights and dignity of their people or group. The enemy of the movement or the organization is the real terrorist, many sites insist, and 'our violence is dwarfed in comparison to his aggression' is a routine slogan. Terrorist rhetoric tries to shift the responsibility to the opponent, displaying his brutality, his inhumanity, and his immorality. The violence of the 'freedom' and 'liberation' movements is dwarfed in comparison with the cruelty of the opponent. The third rhetorical tactic is to emphasize weakness. The organizations attempt to substantiate the claim that terror is the weapon of the weak. As noted earlier, despite the ever-present vocabulary of 'the armed struggle' or

'resistance,' the terror sites avoid mentioning or noting how they victimize others. On the other hand, the actions of the authorities against the terror groups are heavily stressed, usually with words such as 'slaughter,' 'murder,' 'genocide,' and the like. The organization is constantly being persecuted, its leaders are subject to assassination attempts and its supporters massacred, its freedom of expression is curtailed, and its adherents are arrested. This tactic, which portrays the organization as small, weak, and hunted down by a power or a strong state, turns the terrorists into the underdog.

Finally, some of the terrorist sites are replete with the rhetoric of non-violence, messages of love of peace, and of a non-violent solution. Although these are violent organizations, many of their sites claim that they seek peaceful solutions, diplomatic settlements, or arrangements reached through international pressure. Terrorist rhetoric on the Internet tries to present a mix of images and arguments in which the terrorists appear as victims forced to turn to violence to achieve their just goals, in the face of a brutal, merciless enemy, devoid of moral restraints. Demonizing the enemy, playing down the issue of terror victims, shifting blame for the use of violence to the enemy, and proclaiming peace-loving messages are strategies utilized on most terror sites.

Whom do the Internet terrorists target at their sites? Are they appealing to potential supporters, to their enemies (namely the public who is part of the opposing socio-political community in the conflict), or are they targeting international public opinion? An analysis of their contents indicates an attempt to approach all three audiences. Reaching out to supporters is evinced from the fact that the sites offer appropriate items for sale, including printed shirts, badges, flags, and video and audiocassettes. The slogans at these sites also appeal strongly to the supporter public. Of course, the sites in local languages target these audiences more directly. These sites include much more detailed information about recent activities of the organizations and elaborate in detail about internal politics (the relationship between local groups). But an important target audience, in addition to supporters of the organizations, is the international 'bystander' public and surfers who are not involved in the conflict. This is evident from the presentation of basic information about the organization and the extensive historical background material (with which the supporter public is presumably familiar). Similarly, the sites make use of English in addition to the local language of the organization's supporters. Most of the sites offer versions in several languages in order to enlarge their international audience. The Basque

movement site offers information in Castilian, German, French, and Italian; the MRTA site offers Japanese and Italian in addition to its English and Spanish versions. The Uzbeki site offers information in Arabic, English and Russian. Judging from the content of many of the sites, one might also infer that journalists constitute another bystander target audience. Press releases by the organizations are often placed on the websites. The detailed background information might also be useful for international reporters. One of Hizbollah's sites specifically addresses journalists and invites them to interact with the organization's press office via email. Approaches to the 'enemy' audiences are not as clearly apparent from the content of many sites. However, in some sites the desire to reach this audience is evident by the efforts to demoralize the enemy or to create feelings of guilt. The organizations try to utilize the websites to change public opinion in their enemies' states, to weaken public support for the governing regime, to stimulate public debate, and of course to demoralize the enemy. A good example is the following declaration of a Hizbollah leader: "By means of the Internet Hizbollah has succeeded in entering the homes of Israelis, creating an important psychological breakthrough" (Ibrahim Nasser al-Din, from the Internet site of the organization, quoted in Yediot Aharonot, 16 Dec 1998, p. 7).

The instrumental uses of the Internet by terrorism

Denning (2000) distinguishes between three forms of political activity on the Internet: activism, hacktivism, and cyberterrorism. The first category, activism, refers to normal, non-disruptive use of the Internet in support of an agenda or cause. Operations in this area includes browsing the Web for information, constructing Web sites and posting materials on them, transmitting electronic publications and letters through e-mail, and using the Net to discuss issues, form coalitions, and plan and coordinate activities. The second category, hacktivism, refers to the marriage of hacking and activism. It covers operations that use hacking techniques against targeted Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are Web sit-ins and virtual blockades, automated e-mail bombs, Web hacks, computer break-ins, and computer viruses and worms. The final category, cyberterrorism, refers to the convergence of cyberspace and terrorism (to be discussed in the next section)

There is a general progression toward greater damage and disruption from the first to the third category, although that does not imply an increase of political effectiveness. Although the three categories of activity are treated separately, the boundaries between them are somewhat fuzzy. For example, an e-mail bomb may be considered hacktivism by some and cyberterrorism by others. Also, any given actor may conduct operations across the spectrum. For example, a terrorist might launch viruses as part of a larger campaign of cyberterrorism, all the while using the Internet to collect information about targets, coordinate action with fellow conspirators, and publish propaganda on Web sites. Thus, while the paper distinguishes activists, hacktivists, and terrorists, an individual can play all three roles.

The Internet may serve terrorist as an excellent source of instrumental information. One way of viewing the Internet is as a vast digital library. The World Wide Web alone offers about a billion pages of information, and much of the information is free. Terrorist may from the Internet. learn about targets, their schedules, their locations, their timetables. The website operated by the Muslim Hackers Club reportedly featured links to US sites that purport to disclose sensitive information like code names and radio frequencies used by the US Secret Service. The same website offers tutorials in viruses, hacking stratagems, network “phreaking” and secret codes, as well as links to other

militant Islamic and cyberprankster web addresses. Recent targets that terrorists have discussed include the Centers for Disease Control and Prevention in Atlanta; FedWire, the money-movement clearing system maintained by the Federal Reserve Board; and facilities controlling the flow of information over the Internet. Terrorists have access, like many Americans, to imaging data on potential targets, as well as maps, diagrams, and other crucial data on important facilities or networks. Imaging data can also allow terrorists to view counterterrorist activities at a target site. One captured al Qaeda computer contained engineering and structural architecture features of a dam, enabling al Qaeda engineers and planners to simulate catastrophic failures (Gellman, 2002)

With regard to gathering information through the Internet, on 15 January 2003 Defense Secretary Donald Rumsfeld observed that an al Qaeda training manual recovered in Afghanistan said, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy" ("Citing Al Qaeda Manual, Rumsfeld Re-Emphasizes Web Security," *InsideDefense.com*, http://www.insidedefense.com/, 15 January 2003).

There are numerous tools that help with collection, including search engines, e-mail distribution lists, and chat and discussion groups. Many Web sites offer their own search tools for extracting information from databases on their sites. Moreover, terrorists can use the Internet to learn about counter-terrorism: Word searches of online newspapers and journals allow a terrorist to study the means designed to counter his actions, or the vulnerabilities of these measures. For example, recent articles reported on attempts to slip contraband items through security checkpoints. One report noted that at Cincinnati's airport, contraband slipped through over 50 percent of the time. A simple Internet search by terrorists would uncover this shortcoming, and offer the terrorists an embarkation point for their next operation. Several reports in various Internet sites noted that US law enforcement agencies were tracing calls made overseas to al Qaeda cells from phone cards, cell phones, phone booths, or Internet-based phone services. Exposing the targeting techniques of law enforcement agencies allows the terrorists to alter their operating procedures.

Terrorists may use the Internet to provide specific instructions to fellow terrorists including maps, photographs, directions, codes and technical details of how to use

explosives. A recent example is the deadly bomb attack in Finland, 2002. For months, the brilliant chemistry student who called himself RC had been discussing bomb-making techniques with other enthusiasts on a Finnish Internet Web site devoted to bombs and explosives. Sometimes he posted queries on topics like manufacturing nerve gas at home. Often he traded information with the site's moderator, who used the screen name Einstein and whose message carried a picture of his own face superimposed on Osama bin Laden's body, complete with turban and beard. Then he set off a bomb that killed seven people, including himself, in a crowded shopping mall. The Web site used by RC, known as the Home Chemistry Forum, was shut down by its sponsor, a computer magazine called Mikrobitti. But a backup copy, with postings by teenagers who used names like Ice Man and Lord of Fire, was immediately posted again, on a read-only basis.

The practice of steganography, which involves hiding messages inside graphic files, is a widespread art among criminal and terrorist elements. Hidden pages or phrases can be coded instructions for terrorist operatives and supporters. Al Qaeda used prearranged phrases and symbols to direct its agents (Thomas, 2003). An icon of an AK-47 can appear next to a photo of Osama bin Laden facing one direction one day, and another direction the next. The color of icons can change as well. Messages can be hidden on pages inside sites with no links to them, or placed openly in chat rooms (Welch, 2002). In addition, it is possible to buy encryption software for less than $15. Cyberplanners gain an advantage in hiding their messages via encryption. Sometimes the messages are not even hidden in a sophisticated manner. Al-Jazeera television reported that Mohammed Atta's final message (another advantage of the Internet—the impossibility of checking sources) to direct the attacks on the Twin Towers was simple and open. The message purportedly said, "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." (Melman, 2002). The reference to the various faculties was apparently the code for the buildings targeted in the attacks.

Recent report from U.S. officials indicates that terrorists' use of the Web for communication and coordination through the use of encrypted messages is widespread, with numerous sites -- many of which are unaware of the use to which they are being put -- serving as conduits for terrorist conspiracies. Bin Laden's al Qaida and other terrorist groups have reportedly used encryption programs available free on the Web, as well more powerful anti-spy software purchased on the open market. In addition to terrorist sites, the World Wide Web also contains dozens of sites run by domestic white supremacist and militia groups, supporters of terrorist organizations. Many of these sites link to other Web pages that actually provide information on how to build bombs as well as instructions for making dangerous chemical and explosive weapons. Many of these sites post the "Terrorist's Handbook" and "The Anarchist Cookbook" which offer detailed instructions of how to construct a wide range of bombs. Finally, many terrorist sites are used for the solicitation of funds and donations, the recruitment of new members and supporters, and for guiding and directing activists.

More evident is the use of the Internet as an instrumental channel of communication among terrorists: terrorists use simple measures to communicate and coordinate their activities. Back in 1996, the headquarters of the mega-terrorist Bin Laden in Afghanistan was equipped with computers and communications equipment. Egyptian "Afghan" computer experts were said to have helped devise a communication network that used the Web, e-mail, and electronic bulletin boards. Hammas activists have been said to use chat rooms and e-mail to plan operations and coordinate activities, making it difficult for Israeli security officials to trace their messages and decode their contents. It is widely believed that bin Laden and other terrorists use encryption programs – which scramble data or messages into existing pictures that can only be unlocked with a code known only to the recipient – to plan terrorist activities on the internet and relay messages to followers, and there has been a report that two computers recovered from Kabul and apparently in use at an al-Qaeda office contained files protected by encryption. Thomas (2003) argues that the Internet was used to the terrorist attacks of September 11: Computers seized in Afghanistan reportedly revealed that al Qaeda was collecting intelligence on targets and sending encrypted messages via the Internet. As recently as 16 September 2002, al Qaeda cells operating in America reportedly were using Internet-based phone services to communicate with cells overseas. These incidents indicate that

the Internet is being used as a "cyberplanning" tool for terrorists. It provides terrorists with anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options.

Since 9/11, US sources have monitored several websites linked to al Qaeda that appear to contain elements of cyberplanning:

- alneda.com, which US officials said contained encrypted information to direct al Qaeda members to more secure sites, featured international news on al Qaeda, and published articles, fatwas (decisions on applying Muslim law), and books.
- assam.com, believed to be linked to al Qaeda (originally hosted by the Scranton company BurstNET Technologies, Inc.), served as a mouthpiece for jihad in Afghanistan, Chechnya, and Palestine.
- almuhrajiroun.com, an al Qaeda site which urged sympathizers to assassinate Pakistani President Musharraf.
- qassam.net, reportedly linked to Hamas.
- jihadunspun.net, which offered a 36-minute video of Osama bin Laden.[2]
- 7hj.7hj.com, which aimed to teach visitors how to conduct computer attacks.[3]
- aloswa.org, which featured quotes from bin Laden tapes, religious legal rulings that "justified" the terrorist attacks, and support for the al Qaeda cause.[4]
- drasat.com, run by the Islamic Studies and Research Center (which some allege is a fake center), and reported to be the most credible of dozens of Islamist sites posting al Qaeda news.
- jehad.net, alsaha.com, and islammemo.com, alleged to have posted al Qaeda statements on their websites.
- mwhoob.net and aljehad.online, alleged to have flashed political-religious songs, with pictures of persecuted Muslims, to denounce US policy and Arab leaders, notably Saudi.[5]

Do the terror organizations try to enroll supporters through the network? The power of the Internet to mobilize activists is illustrated by the arrest of Kurdish terrorist leader Abdullah Ocalan. When Turkish forces arrested Ocalan, Kurds around the world responded with demonstrations within a matter of hours. This response should be attributed to the Internet and Web. Tsfati and Weimann's analysis of the sites revealed a few attempts to enlist new recruits into an active circle of support, but there was no attempt to mobilize visitors for any actual violence. Kahane Lives (in which the

suggestion appears under the title 'How can I help the struggle: A few suggestions'); the Shining Path ('Action alert: What you can do'); the Basque movement; and the IRA site seeking economic support (including a page for contributions through credit cards) are examples of pages seeking readers' active support. The Zapatista site calls on its visitors to assist the struggle in several ways: to approach members of the Mexican government (the site offers links to the e-mail address of Ernesto Zedillo, the President of Mexico), and to 'send letters of support to ENLZ or local refugees. Educate your friends… Join protest marches outside embassies or diplomatic missions of Mexico near you, or organize such a rally yourself... Send humanitarian aid to Mexico (link to humanitarian organizations)… Donate money to the organization.' In contrast to the absence of appeals for active violence, there is a highly conspicuous effort at many terror sites to obtain supporters for non-violent activity, especially through the signing of petitions.

The Internet can be used as an effective recruiting tool. Individuals with sympathy for a cause can be converted by the images and messages of terrorist organizations, and the addition of digital video has reinforced this ability. Images and video clips are tools of empowerment for terrorists. More important, net access to such products provides contact points for men and women to enroll in the cause, whatever it may be. Current versions of web browsers, including Netscape and Internet Explorer, support JavaScript functions allowing Internet servers to know which language is set as the default for a particular client's computer. Hence, a browser set to use English as the default language can be redirected to a site optimized for publicity aimed at Western audiences, while one set to use Arabic as the default can be redirected to a different site tailored toward Arab or Muslim sensibilities. This allows recruiting to be audience- and language-specific, enabling the web to serve as a recruiter of talent for a terrorist cause. Recently, the Chechen website qoqaz.net, which used to be aimed strictly against Russian forces operating in Chechnya, changed its address to assam.com, and now includes links to Jihad in Afghanistan, Jihad in Palestine, and Jihad in Chechnya. Such sites give the impression that the entire Islamic world is uniting against the West, when in fact the site may be the work of just a few individuals.

Though no direct calls for violence were found, some of the content on the websites could be viewed as encouraging violence indirectly. The Hamas site included calls for Jihad ('Jihad is victory or martyrdom,' 'an eye for an eye,' 'the Jihad will

continue till judgment day'). Of course, the legitimization and justification of violence can also be interpreted as an indirect call for violence. Glorification of martyrs (and the very use of the word "martyr"), for example, signals that the perpetrators of violence are rewarded. However, as mentioned above, this is only the subtext. Most sites' contents ignore violence, and some of the organizations even imply that they seek non-violent solutions.

The Internet can be used to raise funds. According to Thomas (2003), the Internet is used "to put together profiles": Internet user demographics allow terrorists to target users with sympathy toward a cause or issue, and to solicit donations if the right "profile" is found. Usually a front group will perform the fundraising for the terrorist, often unwittingly. E-mail fundraising has the potential to significantly assist a terrorist's publicity objectives and finances simultaneously. The Sunni extremist group Hizb al-Tahrir uses an integrated web of Internet sites from Europe to Africa to call for the return of an Islamic caliphate. The website states that it desires to do so by peaceful means. Supporters are encouraged to assist the effort by monetary support, scholarly verdicts, and encouraging others to support jihad. Bank information, including account numbers, is provided on a Germans site, www.explizit-islam.de. The fighters in the Russian breakaway republic of Chechnya have used the Internet to publicize banks and bank account numbers to which sympathizers can contribute. One of these Chechen bank accounts is located in Sacramento, California, according to a Chechen website known as amina.com.

Fighting back: Responses to terrorism in the Internet

Responding to terrorist Web sites is an extremely sensitive and delicate issue since most of the rhetoric disseminated on the Internet is considered protected speech under the First Amendment. Furthermore, although Web sites belonging to terrorist groups are public, the FBI is precluded from keeping files on them. Agents may surf the Internet but they cannot save material from a Web site on a regular basis unless they are conducting a criminal investigation.

In February 1998, Attorney General Janet Reno unveiled plans to establish a new FBI command center to fight "cyber attacks" against the nation's critical computer networks. In October 2001 U.S. House of Representatives approved an anti-terrorism bill that gave law enforcement officials expanded surveillance powers to monitor Internet behavior and e-mail. After the towers of the World Trade Center collapsed in lower Manhattan, FBI agents were already visiting the offices of Internet service providers (ISPs), network providers, and email vendors around the country in search of those who perpetrated the attacks. The tool they used to conduct that investigation was the controversial email surveillance system, Carnivore (Krause, 2001). The system forces Internet service providers to attach a black box to their networks - essentially a powerful computer running specialized software - through which all of their subscribers' communications flow. In traditional wiretaps, the government is required to minimize its interception of non-incriminating - or innocent - communications. But Carnivore does just the opposite by scanning through tens of millions of emails and other communications from innocent Internet users as well as the targeted suspect. To use an analogy, Carnivore is like the telephone company being forced to give the FBI access to all the calls on its network when it only has permission to seek the calls for one subscriber.

According to the FBI, Carnivore is designed to work "much like commercial 'sniffers' and other network diagnostic tools used by ISPs every day, except that it provides the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. Basically, all Internet traffic is broken down into bundles of information called "packets." Carnivore works as the equivalent of a telephone wiretap for the Internet, looking at each of these packets and recording the

ones that relate to the matter or suspect under investigation. Carnivore can be configured to do one of several things: it can record all of the email messages sent to and from a specific email account. It can record all of the network traffic to and from a specific IP address. It can record all of the email headers (i.e. TO and FROM addresses) sent to and from a specific email account. It can record all of the servers, webpages, or FTP files visited by a particular IP address. And it can track everyone who accesses a particular webpage or FTP file.

Another measure is direct assault on terrorist websites: recently US officials were searching the Internet for the reappearance of alneda.com, a website used as a "mouthpiece" by al Qaida terrorists. It was registered in Singapore and appeared on web servers in Malaysia and Texas before it was taken off at the request of US officials. However, one should consider that the fear that terrorism inflicts can be and in the past has been manipulated by politicians to pass questionable legislation, undermining individual rights and liberties, that otherwise wouldn't stand a chance of being accepted by the public. What are the trade-offs of various counter-measures in terms of security versus privacy and freedom of expression?

Legislative proposals in response to the terrorist attacks of September 11, 2001 were introduced less than a week after the attacks. President Bush signed the final bill, the USA-PATRIOT Act, into law on October 26th. This law introduced legislative changes that significantly increased the surveillance and investigative powers of law enforcement agencies in the United States. Though the Act makes significant amendments to over 15 important statutes, it was introduced with great haste and passed with little debate, and without a House, Senate, or conference report. As a result, it lacks background legislative history that often retrospectively provides necessary statutory interpretation. The Act was a compromise version of the Anti-Terrorism Act of 2001 (ATA), a far-reaching legislative package intended to strengthen the nation's defense against terrorism. The ATA contained several provisions vastly expanding the authority of law enforcement and intelligence agencies to monitor private communications and access personal information. The final legislation included a few beneficial additions from the Administration's initial proposal: most notably, a so-called sunset provision (which provides that the sections of the act automatically expire after a certain period of time, unless they are explicitly renewed by Congress) on some of the electronic

surveillance provisions, and an amendment providing judicial oversight of law enforcement's use of the FBI's Carnivore system. However, the USA-PATRIOT Act retains provisions appreciably expanding government investigative authority, especially with respect to the Internet.

Those provisions address issues that are complex and implicate fundamental constitutional protections of individual liberty, including the appropriate procedures for interception of information transmitted over the Internet and other rapidly evolving technologies. The implications for online privacy are concerning. The Act increases the ability of law enforcement agencies to authorize installation of pen registers and trap and trace devices, (a pen register collects the outgoing phone numbers placed from a specific telephone line, a trap and trace device captures the incoming numbers placed to a specific phone line--a caller-id box is a trap and trace device), to authorize the installation of such devices to record all computer routing, addressing, and signaling information. The new legislation redefined a pen register as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." A trap and trace device is now "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source or a wire or electronic communication."

By expanding the nature of the information that can be captured, the new law clearly expanded pen register capacities to the Internet, covering electronic mail, Web surfing, and all other forms of electronic communications. The full impact of this expansion of coverage is difficult to assess, as the statutory definitions are vague with respect to the types of information that can be captured and are subject to broad interpretations. The fact that the provision prohibits the capture of "content" does not adequately take into account the unique nature of information captured electronically, which contains data far more revealing than phone numbers, such as URLs generated while using the Web which often contain a great deal of information that cannot in any way be analogized to a telephone number. Although the FBI, prior to the enactment of the USA-PATRIOT Act, compared telephone calls to Internet communications to justify invocation of the existing pen register statute to authorize the use of its controversial

Carnivore system, whether the law as then written in fact granted such authority remained an open and debatable question.

When the FBI's use of Carnivore was revealed in July 2000, there was a great deal of concern expressed by members of Congress, who stated their intent to examine the issues and draft appropriate legislation. To facilitate that process, former Attorney General Reno announced that issues surrounding Carnivore would be considered by a Justice promised report had not been released when Ms. Reno left office, and Attorney Department review panel and that its recommendations would be made public. As a result of the delay, Congress does not yet have the benefit of the promised findings and recommendations. Because Carnivore provides the FBI with access to the communications of all subscribers of a monitored Internet Service Provider (and not just those of the court-designated target), it raises substantial privacy issues for millions of Internet users.

Recently, a revised version of the Patriot Act was prepared. This version, labeled informally as "PATRIOT II." And titled the "Domestic Security Enhancement Act of 2003," expands surveillance power, increases government access to private data, and expands the definition of terrorist activities. “We're still reeling from the original USA-Patriot Act's impact on civil liberties and now the government wants more," said Cindy Cohn, the Legal Director of EFF (Electronic Foundation Frontier). "Where is the evidence that the law passed less than two years ago is insufficient? When will Congress draw the line and say 'this much of our civil liberties you've taken under the guise of terrorism -- you may have no more'?" The EFF attempted to document “the chilling effect that responses to the terrorist attacks of September 11, 2001, have had on information availability on the Internet as well as some sense of the effect on people trying to provide this information” (see EFF website, at www.eff.org). This is demonstrated by EFF’s list of (a) Websites Shut Down by US Government; (b) Websites Shut Down by Other Governments; (c) Websites Shut Down by Internet Service Provider; (d) Websites Shut Down or Partially Removed by Website Owner; and (e) US Government Websites that Shut Down on Removed Information.

Additional criticism on PATRIOT II came from ACLU – American Civil Liberties Union. ACLU argued that that the new "anti-terrorism" legislation goes further than the USA PATRIOT Act in eroding checks and balances on Presidential power and

contains a number of measures that are of questionable effectiveness, but are sure to infringe on civil liberties. "The new Ashcroft proposal threatens to fundamentally alter the Constitutional protections that allow us to be both safe and free," said Timothy H. Edgar, an ACLU Legislative Counsel. "If it becomes law, it will encourage police spying on political and religious activities, allow the government to wiretap without going to court and dramatically expand the death penalty under an overbroad definition of terrorism" (see ACLU website, at www.aclu.org).

Conclusion

The Internet may be the most perfect embodiment of the democratic ideals of free speech, open communication, and the "marketplace of ideas" that has ever existed. As the American Supreme Court has written, online "any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox." Unfortunately, freedom on the Internet is far from secure - in fact, it is under challenge from numerous directions, as the present article attempted to show.

The Internet is clearly changing the landscape of political discourse and advocacy. It offers new and inexpensive methods for collecting and publishing information, for communicating and coordinating action on a global scale, and for reaching out to world public opinion as well as decision makers. The Internet benefits individuals and small groups with few resources as well as organizations that are large or well-funded. It facilitates activities such as educating the public and media, raising money, forming coalitions across geographical boundaries, distributing petitions and action alerts, and planning and coordinating events on a regional or international level. It allows activists in politically repressive states to evade government censors and monitors. It is inexpensive to use and increasingly pervasive, with an estimated 250 million on-line. The Internet offers several channels whereby advocacy groups and individuals can publish information (and disinformation) to further policy objectives. Thus the Internet could have become a peaceful and fruitful forum for the resolution of conflicts. And yet, as this article reveals, it has become also a useful instrument for terrorists.

Modern terrorists use the Internet for various functions, from communicative purposes such as propaganda and distribution of information to instrumental uses such as recruitment, co-ordination of actions, hacktivism, and cyberterrorism. Many violent groups with a long record of victimization, bloodshed, and destruction have entered the Internet. Their use of this liberal, free, easy-to-access medium is indeed frightening. The September 11, 2001 attacks by Bin Laden's terrorists promoted the fear and the call for radical counter measures. And yet, one should consider that the fear that terrorism inflicts can and has in the past been manipulated by politicians to pass questionable legislation, undermining individual rights and liberties, that otherwise wouldn't stand a chance of being accepted by the public. It is important to assess the real threat posed by terrorist groups using the new information technology, keeping in mind that governmental action against it could easily go beyond acceptable limits.

Across a wide range of battlefields, privacy is on the retreat. Many high-tech surveillance tools that were deemed too intrusive before September 11, including the FBI's "Carnivore" Internet eavesdropping system, are being unleashed. Pre-attack legislation aimed at protecting people from unwanted privacy invasions has been shelved, while new anti-terrorism laws give the authorities broad new powers to wiretap, monitor and invade Internet activity. These developments could wind up having profound implications for democracies and their values, adding heavy prices in terms of civil liberties to the destructive effects of terrorism in the Internet.

References

Denning, D. (2000). “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy”. http://www.terrorism.com/documents/denning-infoterrorism.html.

Gellman, B. 2002. “FBI Fears Al-Qaeda Cyber Attacks,” *San Francisco Chronicle*, 28 June 2002, pp. 1, 10.

Jenkins, Brian. 1975. International Terrorism. Los Angeles: Crescent Publication.

Krause, Jason. 2001. New Tools Sought to Track Terror Online, *Chicago Tribune* (15 October 2001.

Melman, Y. 2002. “Virtual Soldiers in a Holy War,” *Ha’aretz*, http://www.haaretz.com, 17 September 2002.

Schmid, Alex. 1983. Political Terrorism. N.J: Transaction Books.

Schmid, Alex, and Jongman, Albert, J. 1988. Political Terrorism. Amsterdam: North-Holland Publishing.

Thomas, Timothy, L., 2003. Al Qaeda and the Internet: The Danger of “Cyberplanning” *Parameters*, Spring, pp. 112-23.

Tsfati, Yariv and Weimann, Gabriel, 1999. "Terror on the Internet", Politika, 4: 45-64 (Hebrew).

Tsfati, Yariv and Weimann, Gabriel, 2002. "WWW.Terrorism.com: Terror on the Internet", Studies in Conflict and Terrorism 25(5): 317-332.

Weimann, Gabriel. Winn, Conrad. 1994. The Theater of Terror. New York: Longman Publication.

Weimann, Gabriel, 1999. The Theater of Terror: The Challenge for Democracy. In R. Cohen-Almagor (ed.), Basic Issues in Israeli Democracy. Tel Aviv: Sifriyat Poalim (Hebrew).

Weimann, Gabriel, 2004. WWW.Terror.Net: How Modern Terrorism Uses the Internet, Special report, Washington DC: United States Institute of Peace.

Weimann, Gabriel, 2005. "How Terrorists Use the Internet", Journal of International Security Affairs, 8: 91-105.

Weimann, Gabriel and Tsfati, Yariv, 2002. "WWW.Terror: Terror on the Internet", Studies in Conflict and Terrorism,

Welch, M. T., 2002. “Accumulating Digital Evidence is Difficult,” *The Post Standard*, 11 September 2002, pp. D-9, 11.