CHAPTER FOURTEEN

CYBERTERROR A LA TURCA

MURAT AKSER AND BANU BAYBARS-HAWKS

Introduction

Cyberspace has its share of attacks by Turkish hacker groups. Because of the extensive fear of immediate cyberterror, Turkish hacker movements are feared and called terrorists by western media. Attacks by Turkish hackers on sites criticizing Islam and Turkey have been common since 9/11. This paper aims to identify and classify the thematic concerns of the kind of attacks by these hackers and argue that these activities are not necessarily terrorist acts, but essentially discursive activities. The hackers work in groups in their defacing, i.e. changing the appearance of the site. They have patriot names like Ayyıldız team or Bozkurts. Their action may be ignited by Turkish-Greek relations, the news of Turkish soldiers' deaths, a soccer game between Turks and Serbs or an event such as the Danish caricature crisis. The sites they attack are international brands like SONY to reach the largest audience possible. The intent of their actions is not to inflict financial, but rather to promote a universal message of brotherhood. Hence a new definition of cyberterror, that of ideological hacking, is needed to describe the actions of these groups.

Cyberterrorism: Definitions

Terrorism is at the intersection of radicalism and technology. The main purpose of most terrorist groups today is to create sub-identities, and to this end, these groups highlight ethnic differences. In the past, the "enemy" could be defined or confined geographically. But now, there are no geographical boundaries confining the "enemy" because the enemy is taking advantage of the blessings of technology. Terrorism, with its new face, is more dangerous because its origin is not certain and may not be related to any nation-state. Today's terrorists do not need planes, bombs

and other fire-armed weapons to attack. They can send viruses to computer systems of critical importance and paralyze the military, political and economic resources of one country, or even a continent.

The increasing presence of terrorist organizations on the Net and terror in cyberspace are some of the most important problems currently. Yonah Alexander, a terrorism expert at the Potomac Institute, warns that there will be a move towards the use of non-conventional weapons, such as biological, chemical, nuclear and cyberterrorism, "whereby perpetrators will try to distrupt power supplies and air traffic, for example, at the touch of a button" (Alexander and Swetman 2001, 4). The potential threat posed by cyberterrorism has been widely discussed in the mass media, politics, the security community and information technology industry. The fear of this threat is especially pronounced in the public because two of the greatest fears of modern time are combined in the term "cyberterrorism." The fear of random, violent victimization blends well with the distrust and outright fear of computer technology (Weimann 2004).

Cyberspace is an attractive venue for terrorists because it is cheaper and potentially more anonymous than traditional methods. The variety and number of targets are also very large and cyberterrorists can operate remotely, which is especially appealing. "Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retail followers" (Wiemann 2004, 5). Since cyberterrorism has a direct influence on a larger number of people than conventional terrorism it generates more publicity and receives more media attention, which are what terrorists want. Despite all the frenzy surrounding this new type of terror, suprisingly little is known about the characteristics of it and the actual use of the Internet by terrorists. Therefore, it is crucial to define what "cyberterrorism" is.

Cyberterrorism is the convergence of terrorism and cyberspace. It is defined as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning 2000, 1). Additionally, an attack should result in violence against persons or property, or at least cause enough harm to generate fear, to deem it as "cyberterrorism." Serious attacks against strategically important infrastructures can be considered as acts of cyberterrorism. But *attacks that harm nonessential services or that cause a costly nuisance would not fall under the category of cyberterrorism*. The methods that cyberterrorists can use are quite large. According to Golubev (2001, 4):

- various kinds of attacks involving breaking into a network or obtaining control over a network;
- computer viruses, including network worms that modify and destroy information or hinder operation of computer systems;
- logical bombs; codes placed into programs that are activated at a specific time;
- "trojans" that allow executing certain actions without the knowledge of the owner of the compromised system (trojans sending their owner, through the Internet, different data from the infected system, including users' passwords, are widespread at the moment) and that are designed to hinder exchange of information in networks.

The mass media and film industry contribute to the arousal of this fear. In June 2003, the Washington Post was published with this front-page headline: "Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say." In the movie industry, films like *Golden Eye*, *Swordfish, Die Hard 4.0* and a popular TV series *24* are just some of the examples of programs addressing cyberterror. Mass media is also likely to label hacking activities as acts of cyberterrorism. Therefore, it is important to make a distinction between "hacking" and "cyberterrorism." Hacking is defined as "activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software." On the other hand, cyberterrorists' intention is to kill or terrify, while hackers only want to wreak havoc. However, the distinction between hacking and cyberterrorism sometimes blurs if terrorist groups are able to recruit or hire hackers. Hackers can be turned into cyberterrorists, and this transition can be motivated by money or prestige. As young and educated people are brought into the folds of terrorist groups, this new generation will have the talent to execute acts of cyberterrorism.

The United States government, in the aftermath of September 11, has taken the issue of cyberterrorism into serious consideration, and imposed strict regulations on the Net. In the 45 days after the September 11 attacks, the U.S. Congress passed the Patriot Act, a new anti-terrorism law. "Cyberterrorism" is a new legal term described in the Act. According to the Act, cyberterrorism stands for "various forms of hacking and causing damage to protected computer networks of citizens, legal entities or governmental authorities, including damage caused to computer system used by a governmental agency to manage national defense or to assure national security." In 2002, the government passed the Cyber Security

Enhancement Act as part of the Homeland Security Bill. The bill punishes malicious computer hackers who "recklessly" put other lives at risk with a life sentence and permits limited surveillance without a court order when there is an "ongoing attack" on an Internet-connected computer or "an immediate threat to a national security interest" (Cullagh 2002). The Act also expands surveillance power, increases government access to private data, and broadens the definition of "terrorist activities." European countries have also imposed regulations to control cyberspace. For instance, the Cybercrime Convention accepted by the European Council dated November 23, 2001, was the first international treaty discussing legal and procedural aspects of cybercrimes (Convention 2001). The Convention stipulates actions be targeted at national and inter-governmental levels to prevent unlawful hindrance of computer system functions.

According to Weimann (2004, 30), the Internet is attractive for terrorists because it

- is easily accessable,
- is subject to little or no regulation, censorship, or other forms of government control,
- offers access to potentially huge audiences spread throughout the world,
- is anonymous,
- allows for the fast flow of information,
- is interactive,
- is inexpensive to develop and maintan a Web presence,
- is a multimedia environment (the ability to combine text, graphics, audio, and video and to allow users to download films, songs, books, posters, and so forth), and
- presents the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories.

The growing dependence of our societies on information technology has created a new form of vulnerability, giving terrorists the chance to use cyberspace. "The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure" (Weimann 2004, 2).

Based on the facts regarding cyberterrorism, we suggest that the threat posed by it is exaggerated. Cyberattacks on the critical infrastructure systems of nations are not uncommon, but they have not been conducted by terrorists and have not done the kind of damage that would qualify as

cyberterrorism. Given this, why has the issue generated so much interest and attention? There are a couple primary reasons. First of all, cyberterrorism is sexy right now, it captures people's imagination. It continues to be the theme of popular movies, TV shows, and novels. Second, the mass media fails to make a distinction between cyberterrorism and hacking, and describes most hacking activities as acts of cyberterrorism. The third reason is ignorance. Cyberterrorism is composed of two spheres–technology and terrorism–that many people do not fully understand, and therefore, tend to fear. Fourth, some politicans contribute to this fear by using the threat of cyberterrorism to advance their agendas. And a fifth factor is ambiguity about the very meaning of cyberterrorism, which creates confusion in the minds of public and gives rise to countless myths.

The curious case of Turkish hackers

In this paper we start with this research question: Should Turkish hackers' activities be considered as acts of cyberterrorism? How do their activities differ from their western counterparts? Is there a discourse buried under these activities? Actually, naming Turkish hacker activities as terrorism again falls into the debate of whether cyber hacking activities can be named cyberterror at all. Cyberterror, just like conventional modes of terrorism, aims to create awareness, helplessness and fear in the target country's website, and those citizens must be affected by such an attack. Yet, if the direct aim of the attacks is not to frighten, intimidate or cause panic, but something else such as to create awareness, as in the case of Turkish hackers, is it still considered cyberterrorism? It is our opinion that these hacking and defacing activities are not acts of cyberterror but *disruptive discursive hacking activities*.

We analyze these activities using critical discourse analysis. Our main object of analysis is the Turkish hacking group *Ayyıldız Team*. The website of the group provides interesting insight into the discourse behind these cyber disruptions.

The group

The group name attracts special attention because *Ayyıldız* (the Crescent and the Star) is a symbolic name that transcends back to the middle Asia days of Turkish nationalist ethnic mythology. The website http://www.ayyildiz.org/ operates in five different languages including Turkish, English, German, French, and Arabic. The choice of the worlds' most

popular languages is, in part, due to the fact that most Turkish immigrants abroad live in a country where one of these languages is spoken.

The Ayyıldız team, hereafter referred to as AYT, is composed of hackers from all parts of the world, but mostly from industrialized countries that accept software engineers from developing countries and in time grant them citizenship. For example, Batuhan (Australia), Barbaros (Canada), Atakan (USA), Kahraman (France), Cagabey (Switzerland). In its web communiqués the members refer to themselves in military ranks that resemble Turkish army ranks during the war of independence in the 1920s. One of the founding members of the group, Batuna, passed away in 2008, but the group still operates and has even published a book on its operations that is available underground.

Attack activities and styles

Defacing, i.e. changing the appearance of a site, is the most common activity of Turkish hackers. The symbols used, such as the Turkish flag and the photo of Turkey's founder, Mustafa Kemal Ataturk, reflect nationalist ideas. Their reasons for hacking are religious intolerance (defending Islam) and racial discrimination (defending Turks living abroad and protecting Turkey's image abroad).

As for attacking religious intolerance, AYT earned a reputation for itself during the Danish cartoon crisis of 2006 when it hacked multiple websites in Denmark, not with the intention to destroy or damage, but to protest misrepresentations of Islam and Turks. Similarly, the illustrious hacking of the BM site was related to the Palestine-Israeli issue and Israel's attack on Lebanon. Yet the team added "UN watching African people die" as another reason for its attack, thus enlarging its message and vision far beyond Islam and Turkishness to protecting humanity. On its website, AYT also include two additional issues; its rejection of recognizing the Armenian genocide as well as its rejection of support for the Danish based Kurdish Roj TV, which they believe is responsible for attacks against Turkey.

Another attack was on Germany. This time the theme was a rejection of intolerance towards Turks living in the country. Similarly, 500 sites were hacked in Austria as a result of the "Turkish Delight" incident and the Austrian government's support for the PKK. These attacks voiced opposition to an attack on the Turkish embassy and Austrian police complacency. The AYT refers to these attacks as *the siege of Vienna*.

Bulgarian websites were hacked on account of the ATAKA Party's discriminatory policies against the Turkish minority, destruction of

Ottoman monuments, pressures on Bulgarian and Balkan Turks, support for the PKK and the killing of a Turkish fisherman by the Bulgarian coast guard. An Islamic country like Saudi Arabia could not escape a similar fate. Saudi government and university sites were hacked. This time Saudi Arabia was accused of collaborating with American imperialists, operating the holy land for profit, and passing a death sentence for a Turkish youth named Sabri Bogday.

The heaviest attacks were on Greece. The reasons AYT gave for these attacks on its website are numerous ranging from Greece's support for PKK terrorist camps, pressure on Turks living in Macedonia, constant attacks on Turkey by the Greek press, violation of air and sea sovereignty, the Greek coast guard firing on Turkish fishermen, Greece's Cyprus policy, Greece's support for Armenian genocide claims and a reason as broad as the Greek's historical enmity towards Turks. There were attacks on the Greek parliament, media organizations and government sites. The AYT also proudly declares that it provides counter intelligence on Greek cyberterrorist groups that spy on Turkish government sites. This declaration is another reason why we need to differentiate between harmful and benign hackers and label only the harmful ones as terrorists.

For example, the universal and discursive themes of AYT's activities were revealed when the team attacked Israeli government websites criticizing Israel for "constant violation of international law and acting as US frontline in the Middle East" (ayyildiz team website). This attack was coordinated and organized by subgroups within the organization who have nicknames reminiscent of the freedom war of the 1920s. Attacks can also be against a country whose statements (read as discourse) are anti-Turkey. For example, MSN Italy and Italian air forces websites were hacked and the reason AYT gave is that MSN and the air force support the PKK and try to obstruct Turkey's EU bid.

Agenda: The message

There are several layers of discourse in these attacks.

1. These attacks are evoked by a single action, usually a historic moment when Turkish or Islamic pride is hurt and governments are unable to take necessary action on the issue. Such events include the Danish caricature crisis or the Israel-Lebanon crisis.
2. When these attacks start they own larger discursive missions such as refuting Armenian genocide claims or attacking countries for their illicit support for the PKK. This may be the reason that the

Turkish government may not extend a helping hand, or at least refuses to pursue investigations into these activities, thereby passively supporting them.

3. Attackers' use of a special idiom to describe these attacks, such as the word siege, is reminiscent of the Ottoman empires' siege of medieval European castles. Or the word *tekzip*, which means correction, is used to claim that accusations, such as that of the Armenian genocide, are false and that AYT is providing the correct interpretation of an event.
4. There is explicit concern that these attacks are temporary, do not result in monetary loss or loss of any kind, and hence are not terrorist activities. In fact, AYT is proud that it prevents illegal net activity such as child pornography.

Potential Effects

After AYT's cyber attacks on western government and private corporation sites, the official and personal responses to these attacks portrayed the attackers almost exclusively as perpetrators of an "Islamist Terrorist Attack" or as "Turkish terrorists" (Borst 2008, 130). These hackings last around thirty minutes as the group is not installing Trojans or logic bombs, but simply controlling the IP of the websites. The web administrator changes the IP and restores the original pages afterwards. These attacks cause no financial or material loss. There is shock, an angry response from the owners and users of these websites, but their inability to access the website is temporary. On the other hand, the aim of the hackers is that of reaching the largest possible audience and informing them of their ignorance on the subject of Turks and Islam. No irreversible damage is done and a universal message of brotherhood is given.

Conclusion

In the case of Turkish cyber hacking groups the definition of cyberterror does not apply. Instead a new type of cyber activity is defined, that of disruptive discursive hacking used to reveal the concerns of the attackers.

Works Cited

Alexander, Y., and M. S. Swetman. 2000. *Cyber Terrorism and Information Warfare: Threats and Responses*. Transnational Publishers.

Ayyildiz Team Website. http://ayyildiz.org (accessed December 10, 2010).

Borst, S. 2008. Türken-Gang hackt die EU (Turkish network attacks European Union). *Focus,* 29: 130.

Colarik, A. M. 2006. *Cyber terrorism: political and economic implications*. Idea Group, U.S.

Convention on Cybercrime, Budapest, 23.9.2001.

Cullagh, D. 2002. House considers jailing hackers for life. *Cnet News* http://news.com.com/House+considers+jailing+hackers+for+life/2100-1001_3-965750.html (accessed December 14, 2010).

Denning, D. E. 2000. Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23.

Golubev, V. 2004. Cyberterrorism: concept, terms, counteraction. Computer Crime Research Center.

Gomez, J. 2003. Careful: Someone is watching you surf. *Bandwidth Magazine*, November-December, 2003.

Verton, D. 2003. *Black ice: The invisible threat of cyber-terrorism*. Osborne/McGraw-Hill.

Weimann, G. 2004. Cyberterrorism: How real is the threat? Special Report No.119, United States Institute of Peace, December.

—. 2006. *Terror on the Internet: The new arena, the new challenges*. United States Institute of Peace, U.S.