Introduction

Cyberspace has its share of attacks by Turkish hacker groups. Because of the extensive fear of immediate cyber terror, Turkish hacker movements are also 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 clarify these activities not as terrorist 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 can be ignited by Turkish-Greek relations, on the news of Turkish soldiers’ deaths, a soccer game between Turks and Serbs to Danish caricature crisis. The sites they attack are international brands like SONY to reach the maximum amount of audience. The damage they do is not financial but for their universal message of brotherhood. Hence a new definition of cyber terror, that of ideological hacking is needed to identify the concerns of these attacks.

Cyberterrorism: Definitions

Terrorism is at the intersection of radicalism and technology. The main purpose of most terrorist groups today is to create sub-identity and for this reason, to inflict the ethnical differences. In the past, enemy could be defined or confined geographically. But now, there are no certain
geographical boundaries separating the enemy because they are taking an advantage from the blessings of technology. Terrorism, with its new face, is more dangerous because its origin is not certain and has no relation 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 carrying 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 the cyberspace are some of the most important problems nowadays. 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 disrupt 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 is especially promoted 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 more anonymous than traditional terrorism methods. The variety and number of targets are also very large, and cyberterrorist 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 larger number of people than conventional terrorism, it generates more publicity, receives more media attention, which are what terrorists want.

But despite all the frantics surrounding this new type of terror, suprisingly little is known about the characteristics of it and actual use of the Internet by terrorists. Therefore, it is first 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 could be considered as acts of cyberterrorism. But attacks that harm nonessential services or that cause a costly nuisance would not under the category of cyberterrorism. The methods that cyberterrorists could use are quite large:

- various kinds of attacks allowing breaking into the attacked network or to obtain control over the network;

- computer viruses, including network worms that modify and destroy information or hinder operation of computer systems;

- logical bombs; a code placed into the programs and are activated at some 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);

means designed to hinder exchange of information in networks. (Golubev 2001, 4)

The mass media and film industry have contributed to the arousal of this fear. In June 2003, the Washington Post was published with this frontpage headline: “Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say.” In movie industry, films like Golden Eye, Swordfish, Die Hard 4.0 and a popular TV series 24 are just some of the examples. 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 the acts of cyberterrorism.
The United States government, in the aftermath of September 11, has taken the issue of cyberterrorism into serious consideration, and brought strict regulations on the Net. In 45 days after September 11 attacks, the U.S. Congress passed the Patriot Act, the new anti-terrorism law. “Cyberterrorism” has been a new legal term described in the Act. According 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 into the Homeland Security Bill. The bill punishes malicious computer hackers with a life sentence who “recklessly” put other lives at risk 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). It also expands surveillance power, increase government access to private data, and broaden the definition of “terrorist activities.” European countries have also imposed regulations to control the cyberspace. For instance, Cybercrime Convention accepted by European Council dated November 23, 2001 was the first international treaty bringing up legal and procedural aspects of cybercrimes (Convention 2001). The Convention stipulates actions targeted at national and inter-governmental level, directed to prevent unlawful hindrance of computer system functions. The Internet is attractive for terrorists because (Weimann 2004, 30):

- it offers easy access,
- little or no regulation, censorship, or other forms of government control,
- potentially huge audiences spread throughout the world,
- anonymity of communication,
- fast flow of information
- interactivity
- inexpensive development and maintenance of a Web presence
- 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)
- 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 change 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 by now, we can suggest that the threat posed by cyberterrorism has been exaggerated. Cyberattacks on the critical infrastructure systems of the nations are not uncommon, but they have not been conducted by terrorists and have not given the kind of damage that would qualify as cyberterrorism. So, then, why has the issue taken this much interest and attention? There are couple important reasons. First of all, cyberterrorism is sexy right now, it captures people’s imagination, and with this feature, it has been and is 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 the acts of cyberterrorism. The third reason is the ignorance. Cyberterrorism is composed of two spheres – technology and terrorism – that many people do not fully understand and therefore tend to fear. Fourth, some politicians contributed to this fear with their announcements time to time 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: Can Turkish hackers’ activities be considered cyberterrorism? How do its activities differ from its western counterparts? Is there a discourse buried under these activities? Actually naming Turkish hacker activities as terror acts again fall into the debate of whether cyber hacking activities can be named cyber terror at all. Cyber terror just like the conventional mode of terror acts aims to create awareness, helplessness and fear in the target country’s website and those citizens must be effected by such an attack. Yet if the direct aim of the attacks were not to frighten, intimate or cause panic but something else such as create awareness in the case of Turkish hacker is it still considered cyber-terrorism? It is our opinion that these hacking and defacing activities are not acts of cyber terror but disruptive discursive hacking activities.
As a method we intend to analyze these activities using critical discourse analysis. Our main object of analysis is Turkish hacking group Ayyıldız Team. The website of the group provides interesting insight into the discourse behind these cyber disruptions.

a. The Group:

The group names attract special attention such as Ayyıldız (the Crescent and the Star) and Bozkurt (Gray Wolf) which are symbolic names that transcend back to the middle Asia days of Turkish nationalist ethnic mythology. [http://www.ayyildiz.org/](http://www.ayyildiz.org/) operates in five different languages. Turkish, English, German, French, Arabic. The choice of the worlds popular languages are also in part because of the fact that most Turkish immigrants abroad live in a country where one of these languages are spoken.

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

b. Attack Activities and Styles:

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

As for attacking religious intolerance Ayyıldız team got their reputation for the Danish cartoon crisis of 2006 when they hacked multiple websites in Denmark not with the intention to destroy or damage but to protest misrepresentation of Islam and Turks. Similarly the illustrious hacking the BM site was related to Palestine-Israeli issue and Israel attack on Lebanon. Yet the team added “UN watching African people die” as another reason for their attack thus enlarging their message and vision far beyond Islam and Turkishness to protecting humanity. In their website defense they also add two more issues that of the recognition of Armenian
genocide and supporting the broadcasting by Kurdish Roj TV that attacks Turkey in Denmark.

Another attack was on Germany this time the theme was intolerance to Turks living in the country. Similarly 500 sites were hacked in Austria as a result of the ‘Turkish Delight’ incident and Austrian government’s support for PKK, an attack on Turkish embassy and Austrian police complacency. This they call *the siege of Vienna*.

Bulgarian websites were hacked on account of ATAKA Party’s discriminatory policies against Turkish minority, destruction of Ottoman monuments, pressures on Bulgarian and Balkan Turks, support for PKK and killing of a Turkish fisherman by Bulgarian coast guard. An Islamic country like Saudi Arabia could not escape similar fate. Saudi government and university sites were hacked. This time Saudi Arabia was accused of acting with American imperialism, operating holy land for profit, passing a death sentence for a Turkish youth Sabri Bogday. The heaviest attacks were on Greece. The reasons Ayyildiz Team lists on their website are numerous ranging from Greece’s support for PKK having terrorist camps, pressure on Turks living in Macedonia, constant attack on Turkey by Greek press, violation of air and sea sovereignty, Greek coast guard firing on Turkish fishermen, Greece’s Cyprus policy’ Greece’s support for Armenian genocide claims and a reason as wide as historical enmity towards Turks. There were attacks on Greek parliament, media organizations and government sites. The ATY team also proudly declares that they provide counter intelligence on Greek cyber terrorist groups that spy on Turkish government sites. This move is another reason why we have to differentiate between a harmful and benign hackers and call the former terrorist.

For example on the universal and discursive themes of Ayyildiz group’s activities shows itself when they attack Israel government websites baling them for “constant violation of international law and acting as US frontline in the Middle East” (ayyildiz team website). This attack was coordinated and organized with subgroups of the organization with nicknamed reminiscent of freedom war of 1920s. Or an attack could be against a country whose statements (read as discourse) are anti-Turkey. MSN Italy and Italian air forces website were also hacked and the reason AYT gives is that they support PKK and try to prevent Turkey’s EU bid.

c. *Agenda-The Message:*
There are several layers of their discourse in these attacks.
These attacks are evoked by single action, usually a historic moment when Turkish or Islamic pride is hurt and these governments are unable to take necessary action on the issue. Such events include Danish caricature crisis or Israel-Lebanon crisis. When these attacks start they own larger discursive missions such as refuting the Armenian genocide claims or attacking countries for their illicit support for PKK. This may be for reason that Turkish government may extend a helping arm or at least refuse to pursue investigations into these activities thereby passively supporting them. Attackers use a special idiom to describe these attacks words like siege is reminiscent of Ottoman empires siege of medieval European castles. Or the word tekzip, correction, is used to claim that the accusations such as genocide as false and that they are providing the correct interpretation.

There is explicit concern that these attacks are temporary, they do not result in monetary loss or loss of any kind and hence are not terrorist activities. In fact Ayyildiz team is proud that it prevents illegal net activity such as child pornography.

d. Effects:
After Ayyildiz Team’s cyber attacks on western government and private corporation sites, the official and personal responses portrayed the attackers almost exclusively as “Islamist Terrorist Attack” or “Turkish terrorists attack government website” (Borst 2008: 130). These hackings last around thirty minutes as they are not installing Trojans, logic bombs but simply control the IP of the websites. The web admin changes the IP and restore the original pages afterwards. As an effect there is no financial and material loss. There is shock, an angry response from the owners and users of these websites but their inability to access is temporary. On the other hand the aim of the hackers is that of reaching the maximum amount of audience in the target and instruct them of their ignorance on the subject of Turk and Islam. No damage is done and a universal message of brotherhood is given.

Conclusion

In the case of Turkish cyber hacking groups the definition of cyber terror does not apply. Instead a new type of cyber activity is defined that of disruptive discursive hacking to identify the concerns of these attacks.
Works Cited


Ayyildiz Team Website. [http://ayyildiz.org](http://ayyildiz.org)


Cullagh, Declan “House considers jailing hackers for life,”


