AARMS
Vol. 6, No. 4 (2007) 659–671

New way of terrorism:
Internet- and cyber-terrorism

ZSOLT HAIG, LÁSZLÓ KOVÁCS

Miklós Zrínyi National Defence University, Budapest, Hungary

In this paper we show how the terrorist organizations use the possibilities given by the Internet to organize their own activities, to present their organizations and we also show what opportunities they have, by using the net, to execute various attacks.

The traditional way of using terrorism and information technology: "soft" means and methods

If we examine the history and development tendencies of terrorism, we can claim that it has always got accustomed to the development tendencies of the world. It is not any different in our globalizing world either, that is, terrorism is globalised necessarily as well, and its bond to the media is getting tighter and tighter.[1] This bond is even more strengthened that the most up-to-date communications and information systems and networks are available for them as well, by the help of which they can get information important for them in a faster and more effective way as well as can pass them to their target audience.

If we examine the use of information technology for terrorist purposes, we can highlight the following points:

- *the "soft" type of application of information technology*, which refers to the fact that the terrorist organizations and groups use these systems and means not for demolition and impairment but primarily for propaganda activities, for the formation of public opinion, etc.;
- *the "hard" type of application of information technology*, which explicitly refers to cyber warfare methods. Within this framework the goal is to break into computer networks, to restrict the operation of information infrastructures, to cause deficiencies in information, etc. By monitoring and analyzing the terrorist attacks and actions of nowadays, we can claim that the "hard" type of application is, at present, is less widespread than the "soft" one.[2] At present the terrorists are less interested in the disablement of different networks since these networks ameliorate the actual movement possibilities and logistics of the

Received: September 20, 2007

Address for correspondence:
ZSOLT HAIG
Miklós Zrínyi National Defence University
P. O. Box 15, H-1581 Budapest, Hungary
E-mail: haig.zsolt@zmne.hu

aggressors to a great extent. Without these several actions could not even be implemented at all.[3]

From the list above it is apparent that the Internet provides excellent opportunities for the terrorist organizations to build and maintain their networks and to advertise their ideas. The Internet is not controlled by any institution; it is formed by the cooperation of networks controlled independently of each other.

Connecting to the Internet can be achieved in several ways:

- through a modem;[i]
- on Integrated Services Digital Network (ISDN);
- on a hired line;
- on Asymmetric Digital Subscriber Line (ADSL);
- on a cable TV network;
- on a mobile phone, on a regular data channel or through General Pocket Radio Service (GPRS);
- on micro-wave as well as through satellite connection.[4]

The Internet-network, exactly due to its decentralized characteristic, is a very safe communication platform and the information flow on it can be followed and detected in a very difficult way. This has been realized by various extreme groups and political organizations – as well as the terrorist groups –, who try to make use of the possibilities of this technology in some ways. What is more revealing is that while in 1997 merely twelve terrorist websites were counted by experts, now the number of such websites is put between 4, 500 and 10,000.[1]

The advantages of the Internet from the aspects of terrorism:

- *easy accessibility:* anyone can have an Internet access from anywhere, either on a land line or on radio or satellite connection or through WLAN[ii] networks. This way for instance one can get access to the Internet even from the desert;
- *the rules are minimal, there is no censorship:* this is well perceptible from debates going on nowadays about how the Internet could be regulated, thus preventing the spread of the objectionable web sites;
- *the target audience is potentially huge:* access to the given content is unrestricted, the number of those getting access is affected only by the capacity of the server or the bandwidth;
- *anonymity of communication:* due to the problem of detectability it is not known who is communicating with whom at the given time;

[i] Dial-Up

[ii] Wireless Local Area Network

- *information flow is very fast:* as soon as a web page is prepared, it is put on the Internet and from that moment on it is accessible to anyone;
- *its formation is very cheap, it does not require big costs:* its infrastructural background has to be provided only once, which, from that moment on, can be used freely;
- *multimedia environment:* in which possibilities are given (audio, video, still image, text) by which deterrence, propaganda, etc. can be made us of to a significant extent;
- *the traditional mass media regards the Internet as its source more and more:* they often refer to various Internet news portals.

These advantages have been recognized by the terrorists as well and they have been continuously exploiting them. At present more than 40 terrorist organizations operate web pages of which there are some that operate more than one and even in more languages. These terrorist web sites can have various contents, such as:

- the history of the organization (actions so far, organizational changes etc.);
- social and political background on which terrorism is based and on which ideologies are built;
- major terrorist actions executed;
- the CV of leaders, their "heroic" acts;
- founders and heroes (suicide bombers, "martyrs");
- political and ideological goals;
- fervent criticism of the enemy;
- the presentation of debated areas on maps up-to-date information.[5]

The target groups of the terrorist web sites can essentially be divided into three big groups:

1. *the group of actual and potential supporters*, that can be relied upon and that can be further strengthened for the purpose of further support. For this target group on-line web stores are operated where various articles (T-shirts, flags, video- and audio tapes, etc.) can be purchased;
2. *the international public opinion*, whose members are not connected to any terrorist organization, incidentally visiting such web pages as enquirers. By information and propaganda activities that can be found on the web site this target group is informed or incidentally they try to bring them over in the interest of their own cases. Accordingly these web sites appear not only in the local language but also in several world languages. The web site of the ETA, for instance, can be accessed in the Catalan, German, French and Italian languages as well. The foreign journalists can be put into this category, too, for whom easily accessible press releases are provided

so that they can pass on their own aspects and positions on a given issue in a more authentic way. Thus the Hezbollah provides connection even by e-mail to the journalists in the hope of faster and more effective information.

3. *the hostile publics*, against which the terrorist organizations take steps. Towards this audience the goal is, by presenting various terrorist acts, to demoralize the population, to arouse remorse in them, to whet possible debates in the public opinion by which the governmental support can be decreased to a great extent.[5]

It is worth mentioning that from the target audience the children cannot be excluded either, for instance the children web page of the Hamas (www.al-fateh.net, Figure 1) various cartoons and on-line games can be found, by which it is presented how to shoot, to blast, to commit outrages, etc. in a playful way. Thus it is apparent that the future generation cannot be excluded form the potential target groups either, since some time they will become the suicide bombers of the future.

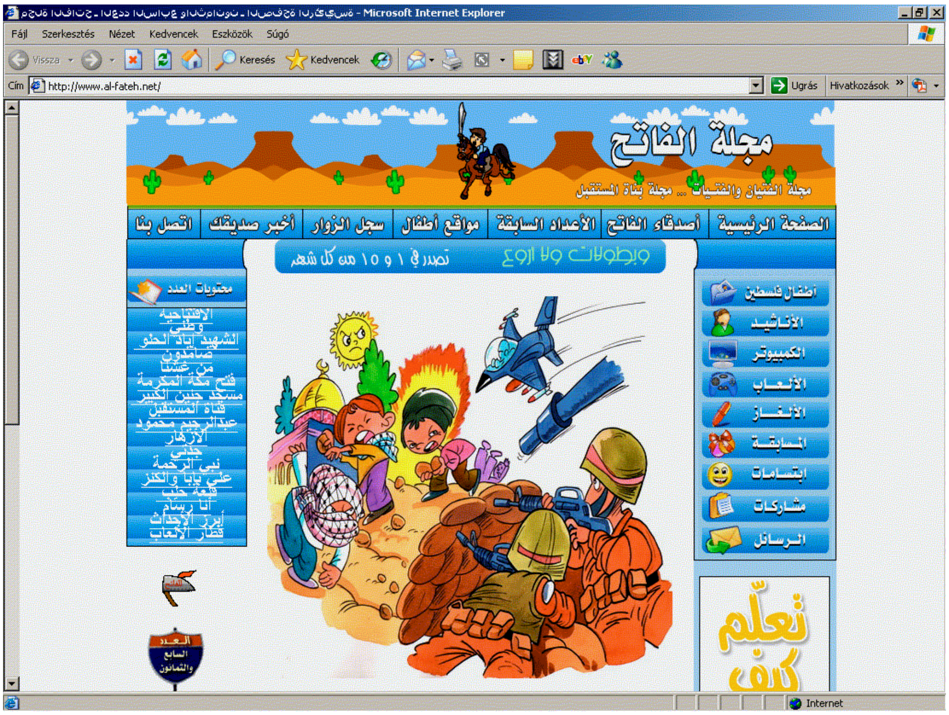

Figure 1. The opening page of the children web page of the HAMAS[6]

The content of the terrorist Internet sites

In the following parts let us see how and for what terrorists use their Internet websites.

From the viewpoint of use with terrorist purposes the Internet can be suitable for the following tasks:

- psychological warfare;
- publicity and propaganda activities;
- data mining;
- collecting donations;
- recruitment and mobilization;
- network-building;
- sharing information;
- command and control (planning and coordination).[5]

Psychological warfare

From the nature of terrorism its psychological connection is obviously resulting from it since by committing various bombing and suicide attacks the goal is not merely destruction, but also the intimidation of the population and keeping them in constant terror. One rather suitable tool of planting constant fear in people is the Internet which is used by the terrorists quite an intensive way. There are several ways to perform psychological warfare through the Internet, such as miscommunication, mailing threats, planting fear by presenting pictures and video recordings, etc. One such characteristic example was the circulation of the video recording of the brutal murder of Daniel Pearl, an American journalist, on various Internet sites.[5]

The Internet is quite a suitable place for psychological pressure since people are terrified of everything that is invisible and incomprehensible for them. An example for this is the possibility of cyber terrorism, that is, the probability of attack in the virtual space (in the informational dimension),[iii] that is, the spread of "cyber-fear".[8] Let us just think what damage a cyber attack can cause for instance in air traffic control, in the computer systems of the stock-market, in the electric supply, etc., since each of these systems are heavily dependent upon the operation of computer networks.

As an example, the Al-Qaeda efficiently combines modern multimedia propaganda and developed communication to reach the goals of refined psychological warfare. Video- and audio recordings, photos and statements can be accessed on several of their websites. The attack against the twin towers of the World Trade Center was presented

[iii] The information warfare (information operations) has their effects in the physical-, in the information- and in the perceptual dimensions to achieve information superiority.

on video with flash animation as a strike against the economic trademark of the USA.[5] All these have proved to be rather efficient and caused widespread fear and insecurity in the public opinion of the world, however, especially in the United States of America.

Publicity and propaganda

The Internet extends the limits of publicity to a great extent and provides safe publicity for the terrorists to spread their ideas. As long as they are unable to address the traditional media – since the statements and ideas of terrorist groups cannot be communicated on TV, on radio or in newspapers, or only in case of very strict censorship – the Internet, on the other hand, provides unlimited opportunities to do this.[8]

Most websites emphasize the restrictions in connection with the freedom of expression and the political prisoners. With these high-sounding statements they try to bring over part of the public opinion that is committed to abolish censorship and to let the political prisoners go free. They emphasize, in every possible way, that to be able to achieve their goals they have no other possibility but violence. They put themselves in the position of freedom fighters that are fighting only for their justice and they see the real terrorist in the enemy. As a result of this they devolve every responsibility to the enemy.

At the same time as armed forces they make use of every possibility to change the violent picture formed about the terrorists. They assert on several websites that they have been looking for the possibilities of peaceful solutions and that their final goal is nothing but diplomatic settlement.[5]

Data mining

The Internet is a huge digital library with more than one billion pages. Most of them are freely accessible and the terrorists are, by choice, interested in them. The majority of these pages contain sensitive data that are quite valuable for an unauthorized user who is interested in them. Several unpublished critical information can be found on the net, such as the 3D vision pictures, ichnography data, etc. of important buildings and institutions. From these they are able to collect important data about various infrastructural institutions (airports, transportation infrastructures, nuclear power stations, electric supply systems, water supply systems, etc.) by open source intelligence (OSI). A wide treasury is supported by an Al-Qaeda handbook according to which 80% of the necessary information can be gathered from public sources, mainly from the Internet.[8]

Since this information is openly accessible, they mean a considerable amount of risk as for the operation of a country. Of course it is not enough only to get the critical information; they also have to be evaluated. By suitable softwares, the terrorists are able to study and analyze the vulnerability and attackability of various institutions, in a given case, to model the scenario of a potential attack.[5] The computer criminals paid by the terrorists map the potential targets by analyzing the open databases and by cracking the secret databases.

Of course the traditional mass media also provides for such critical information, however, the search possibilities of the on-line papers provide faster and more information to a much greater extent than their printed counterparts. Thus the given bodies have to have the emphasized task to inspect the safety of the openly accessible data of the critical infrastructures ensuring the operation of the information society as well as to put an end to great publicity.

Collecting donations

As every political organization, the terrorist groups use the Internet to increase their financial basis to a great extent. The Al-Qaeda has always greatly depended upon the various donations. Global donation networks have been built up to increase their financial basis in a more effective way which are based on various foundations, bodies independent of governments and monetary institutions. Various websites, Internet-based chat rooms and forums have been used to collect donations. For instance, on the webpage of the IRA the visitors can give donations by using their credit cards.

To bring over the supporters they also make use of the possibilities offered by the Internet. Based on on-line questionnaires they gather personal information and by a special question they are able to identify who can be counted as a sympathizer. Then these people are addressed either directly or by e-mail and they can be asked for financial donations for their "just cause".[5]

Recruitment, mobilization

The terrorist websites are used not only to collect financial donations from the sympathizers but also to map and to recruit them. Through these activities they are asked to take a more active part in the execution of the terrorist attacks. The possibilities offered by the multimedia are also used for recruitment. The mapping and getting in touch with those visiting the terrorist sites and those who are interested in them is done through e-mail, by the help of chat sites and by forum sites.

Among the means of recruitment we can find the praising of those who gave their life for the "just cause". The website of the Hamas is full of the photos and names of terrorist martyrs as well as of the dates of the suicide attacks. By this they over-praise those who sacrificed themselves by which they can bring over more people for their plans.[7]

Network-building

Most terrorist organizations – beginning from the Hamas to the Al-Qaeda – have been stepping out of the national frameworks and have become more and more international. There are cells in various parts of the world isolated from each other that are able to keep in touch by the help of the Internet. The Al-Qaeda does not function as a traditional terrorist organization any more. Their members do not live together, they do not hold the trainings together and there are cases when they never even meet each other. They do not need direct contact since they are able to communicate with each other in other ways. Instead of vertical ways of being connected they have shifted to horizontal network communication which significantly encumbers their disclosure. For this the Internet is an excellent means as well since it is extremely fast, it significantly reduces the information transmission time, it has a rather low demand of cost and the information to be transmitted can have a lot of formats (text, still image, motion picture, etc.).

Sharing information

The Internet – as we have all experienced – is the treasury of free access to information. There are several ways to download data of various formats, see the various file sharing systems, forum sites, etc. Thus the Internet is also a free treasury of the means of terror. This way it becomes possible that the training of the terrorists should not be a task executed together.

Anyway, the drilling of the terrorist should not necessarily be imagined on a shooting-ground. Volume 9 of 2004 of the Al-Qaeda publication, the Al Battar (The Sword) provides detailed guidelines for kidnapping. Various methods, potential targets and negotiation strategies are suggested and it also gives advice on how to film decapitation and how to put the video recording on the net. Another on-line publication of the Al Battar is about weapons and their use.[7]

Besides the ones mentioned above there are several other handbooks and guidelines (The Terrorist’s Handbook, The Anarchist’s Cookbook, The Mujahadeen Poisons Handbook, Sabotage Handbook etc.) that can be especially useful drilling materials in skilled circles. Thus nowadays anyone who wants to launch an attack can practically find every necessary information on the Internet, – from the recipes of the home-made explosives through the refuge and information safety techniques to the drilling guidelines.[1]

It may be worth mentioning that the most well-known and most widely used Internet search engine of nowadays, the Google gives more than 10,000 findings to the expression “Terrorist’s Handbook”. Of course these references do not all directly point to the terrorist handbooks, however, this huge number also shows how easy the situation is for the people and groups with harmful intents.

Command and control (planning and coordination)

Finally we have to mention that the planning, organization and control of the terrorist attacks are not performed by the methods that we call traditional either. It is well-known that the organization of the attack of 11 September 2001 was also executed through the Internet. To keep in touch they partly employed encrypted messages sent through sites protected by passwords. The frequency of sending messages was the highest in August 2001. Besides this the terrorist also sent e-mails to each other from public places, through public e-mail providers in which there were ordinary messages and by which they tried to deceive the authorities.[5] The terrorists bought their plane tickets through the Internet and they also got social security numbers and fake driving licenses.

They have used steganography[iv] to hide messages several times. Various commands, the maps and photos of the targets and technical data were hidden behind various pictures and graphics and they were sent to each other.

The new type of application of terrorism and of information technology: "hard" means and methods

In the previous parts we could see that the terrorist organizations also make use of the opportunities provided by information technology. However, from the analyses above it turns out that they do not use the Internet to attack but to get information, to keep in touch, etc. By examining the question, however, the danger arises that the possibilities given by the Internet are used for attacks whose targets may be the critical information infrastructures.

Information terrorism and cyber-terrorism

Besides traditional terrorism, terrorist threats adapt to the new age and thus carry new types of dangers appear that are called information terrorism. Information terrorism is an expression – used in a rather wide sense – which we use for terrorist threats and actions that appear through the information infrastructures, by using them or by assigning exactly them as targets or threatening them. Information terrorism can be manifested in cyber-terrorism as well, since in the majority of the cases such terrorist attacks are executed from the cyber-space or, by using them, exactly in the cyberspace. Thus information terrorism is a collective noun, in which every – even combined with traditional elements – terrorist attack or action is included that intends to reach its goal by the use of some informational infrastructure or by regarding it as a target. As

[iv] Hiding messages into picture files and into texts.

opposed to this, cyber-terrorism is meant for terrorist activities that appear mainly on the Internet or on computer networks and that intend to reach their goals there.

In the case of cyber-terrorism we often hear about and see pictures that seem frightening about server entries and about cracked Internet websites. We often see that, to prove the fact of cracking the perpetrators – we can call them hackers or crackers – re-modify and reorganize the given site, often reminding them of satiric caricatures. The sites modified in face – defaced websites – as well as the damages caused by these, however, are not very significant since the original content and face can be restored within a short amount of time with a relatively short amount of energy. However, the warning sign is there, if the crack of these sites was possible, if the hackers were able to do this, then they are able to enter other, more important sites than these. And if this is the case, or if this knowledge meets an extreme political idea or view, then society is in a really big danger of attacks arriving from the cyberspace, which might as well arrive through infrastructures that are inevitably necessary for our everyday life and for social development.

To sum up all these it can be said that cyber-terrorism is an aggressive and destructive activity appearing at the meeting point of traditional terrorism and cyberspace. They usually mean attacks and threats against the computer networks and computers as well as against the information flowing or stored on them by which the cyber-terror groups or individuals intend to achieve their political or other goals.[9]

The potential means of information terrorism and cyber-terrorism

Means that can be counted as the possible means of information terrorism and cyber-terrorism are the same as we more or less know nowadays in connection with network attacks executed on the Internet. So the basic means of cyber-terrorism are the means performing network attacks by which one can enter a computer network and where the following damages can be caused:

- they keep down resources (memory, disk space, processor capacity);
- loss of data, modification of data;
- hardware error – physical harm;
- their removal requires time and energy.

Some of the means that may be suitable for the attack against networks or for penetration:

Malwares (Malicious Software):

Program type malwares:

- computer viruses and program worms:
- virus development kits;
- Trojan and backdoor programs;

- dialers;
- droppers;
- spy programs;
- keyloggers;
- other harmful programs.

Text type malwares:

- spam;
- hoax;
- Dutch and Spanish lottery winning letters;
- Nigerian cheats;
- phishing, pharming;
- other text type harmful contents.

Other attacks (frequently use of previous mentioned malwares):

- denial of service, distributed (CodeRed, Nimda)
- spamming, viral (see. love-letter);
- flooding (TCP SYN[v] packet);
- man-in-the-middle attack;
- SMTP[vi] backdoor command attack;
- IP address Spoofing attack;
- IP fragmentation attack;
- TCP Session Highjacking;
- information leakage attack;
- JavaScript,- applet attack;
- XSS;[vii]
- zero day exploit.

All these are made especially dangerous since by these means even systems can be attacked which appear in connection with the critical information infrastructures, that is, these crucial systems can be directly attacked.

At the same time it has to be mentioned that these systems can become real victims – and together with this our Western type societies as well – in case if, parallel to the cyber attacks or completing them traditional terrorist attacks are also performed, target our infrastructural systems. This is the case when we can really talk about information terrorism. The targets of information terrorism – that is, a cyber- and traditional attack executed in a complex way – can be the followings:

[v] Transfer Control Protocol Synchronization.
[vi] Simple Mail Transfer Protocol.
[vii] Cross Site Scripting.

- *the energy power, -storage and –transportation infrastructures:* the coal- and oil fuelled, gas work, water-, wind-, solar-, biogas- and nuclear power plants, natural gas and petroleum producer- and refining companies, coal mines, electric energy converters, power-lines, petroleum- and natural gas delivery lines, etc.;
- *the banking and financial infrastructures:* banking networks, trade centers, stock- and produce exchanges, other financial organizations;
- *the water supply systems:* water-purifying plants, reservoirs, water conduit and sewage systems, etc.;
- *the telecommunication and communication systems*: telecommunication and communication means which include computer based networks, softwares, etc.;
- *the transportation infrastructures:* national airlines, airports, public road passenger- and freight transportation companies, road- and highway networks, railway companies, railway networks, water carriage means, etc.;
- *the emergency and disaster recovery infrastructures:* ambulance, police, fire department, health care institutions, disaster recovery services, etc.;
- *the governmental and self-governmental bodies.*

Summary

All in all we can say that the terrorists nowadays are not behind either in knowledge or in infrastructure, what is more, a significant amount of financial donations are appropriated on the development of informational technology. We can find some inconsistencies in this field in case of the Arab terrorists since they use the Internet and other means of modern information technology, for choice; at the same time, their topmost enemy is the embodiment of society based on this modern technology, the United States of America.

At present primarily the so-called “soft” type of use of informational technology has been spread rather than the “hard”, the offensive type of application. Within the “soft” type of use the Internet is used for choice and very effectively on eight areas that overlap each other on more areas.

However, there is a real danger that by the use of information technology on the Internet or through various networks a cyber-attack may occur which, by the implementation of parallel traditional terrorist attacks can regard our informational systems as targets. To avoid such a “hard” – information terrorist – attack there is a need for international anti-terrorist cooperation.

As a final conclusion we have to claim that the governments or bodies that want to act against the terrorist organizations have to start actions in this field, too, they have to map these web pages, they have to monitor the information activities on them all the time and in a given case they have to make them unserviceable. The first steps in this direction have already been taken, several terrorist websites have been cracked by the professionals of the American authorities and by some hackers and thus they are not available.

*

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

References

1. TÁLAS, P.: A terrorizmus elleni küzdelem néhány dilemmájáról. (About some dilemmas of fight against terrorism.) *Hadtudomány,* (2005/4) 194–202.
2. HAIG, Zs.: A terrorizmus új eszközei és módszerei. (The new means and methods of terrorism.) *Felderítő Szemle,* (January 2006) 123–138
3. TAMÁS, P.: *A terrorizmus mint informatikai kihívás.* (Terrorism as an information challenge.) http://21.sz.phil-inst.hu/TamasP/terror.htm
4. HAIG, ZS., VÁRHEGYI, I.: *Hadviselés az információs hadszíntéren*. (Warfare on the information battlefield.) Zrínyi Kiadó, Budapest, 2005.
5. G. WEIMANN: *www.terror.net: How Modern Terrorism Uses the Internet*. Special Report 116. March 2004. United States Institute of Peace.
6. HAMAS children website: http://al-fateh.net
7. T. SPRING, E. KUMLER*:* High-tech terrorism*. PC World Magazine* (2004/39).
8. T. L. THOMAS: Al Qaeda and the Internet: The Danger of "Cyberplanning". *Parameters,* XXXIII/1. (Spring 2003) US: Army War College Quarterly.
9. HAIG, ZS., KOVÁCS, L., VÁNYA, L.: *Információs hadviselés – információs terrorizmus – kiberterrorizmus. Az informatikai biztonság kézikönyve, 3.6. fejezet* (Information Warfare – Information Terrorism – Cyber-Terrorism. The Information Security Handbook, Chapter 3.6.) Verlag Dashöfer, Budapest, 2006.