BILETA

16th BILETA Annual Conference

April 9th - 10th, 2001.
University of Edinburgh, Scotland.

CYBER-TERRORISM : A CALL FOR GOVERNMENTAL ACTION?

VARVARA MITLIAGA
(University of Edinburgh, UK)

I. Introduction.

The great advances in information and communications technology have an unprecedented impact on our society: a considerable percentage of our life and activities has come to depend heavily on information infrastructure. This dependence is very much apparent in both the public and private sectors. Vital factors of public life such as air, road, and railway traffic control, the dissemination of energy like electricity or gas, telecommunication systems like wire and mobile telephony, police or fire dispatch centres, hospitals, government offices and systems controlling key sectors such as national defence, and many more public services are now organised and controlled through the use of computers and networked systems. The situation is not much different in the private sector, computers and the internet are highly involved in the way we work, communicate, buy or sell products, run businesses, control or invest money, educate or entertain ourselves. Banks, stock markets, and other monetary institutions that transfer or handle vast amounts of money base their operation entirely on computer systems.

This great dependence on information technology has created a new form of vulnerability for society, public or private life can be highly disturbed by those who are able to manipulate information technology for illegal purposes. Besides, information technology is widely available and approachable in terms of price for anyone who wants to use it, at least in the developed world. Computers are not inherently good or bad, so they can be either used for moral and legitimate purposes, or manipulated by criminals to pursue their immoral and illegitimate ambitions. The latter has given rise to a new form of criminal behaviour, computer crime, a term comprising all the possible cases where a computer or a network can play a role in a criminal case.

Terrorists constitute one of the criminal groups that are expected to take advantage of information technology, either as a means of enhancing their traditional activity or as a new attractive target against which to launch their attacks. Cyber-terrorism is a recently adopted term used to describe the convergence of cyberspace, the virtual world where computer programs function and data moves, with traditional terrorism[1]. It is a relatively new phenomenon, one of the lot that have emerged in the above described context of dependence on information technology. Notwithstanding its great relevance with computer crime, cyber-terrorism constitutes an indispensable phenomenon worthy of

being analysed on its own. Traditional terrorism has always been a major issue for governments due to its nature, greatly distinct from traditional delinquency, that calls for a separate action. It is a phenomenon with purely ideological dimensions, usually political or religious, that operates by inflicting fear to people and coercing decision-making. Likewise, cyber-terrorism has a different nature and characteristics from the average computer related criminal behaviour. Governments tend to increase their power when they "label" criminals as terrorists and citizens seem willing to accept more abuses of power when a counter-terrorist campaign is in progress[2]. That is why it is important to define cyber-terrorism and have a clear idea of its nature and potential.

The purpose of this paper is to examine and analyse the use of information technology by terrorists, determine what does and what does not constitute cyber-terrorism and the real threat it poses for society, in order to decide whether there is a need for special governmental action targeting in combating it.

II. Traditional terrorism and the use of information technology.

a. An overview of traditional terrorism

Even though terrorism is a phenomenon with a long history[3], there is still a controversy on the definition of the term[4]. Traditional terrorism is a complex phenomenon, it can be roughly described as an act or aggregation of premeditated acts involving criminal violence, intending to intimidate civilian population and coerce governmental decision-making, or, generally, to express disagreement for governmental policies and actions. The basic characteristic of terrorism is the use or threat of violence against persons or property aiming to cause enough harm to attract attention, generate fear, and affect decision-making. Unlike conventional crime, it has its roots on strong ideology, it is basically an effort designed to impose it by illegal and violent means. The most popular ideologies that inspire contemporary terrorist groups are anarchism, far-left communism, neofascism and neonazism, nationalism or national separatism, and religion[5]. This catalogue is not exhaustive, there are other less-strong ideologies whose supporters resort to unconventional ways of defending and imposing them, like for example animal protection, but their intention is rather to intimidate and attract attention than to cause serious damage to property and even more to people. It is anyway debatable whether such groups qualify as terrorist, the decision rather depends on how far they go in using violence and distracting normal life.

It is also important to underline a few other points. One of the enduring axioms of terrorism is that it is designed to generate publicity and attract attention to the terrorists and their cause, media publicity is indispensable for an attack to be successful and attain its scope. Furthermore, attacks are always premeditated and carefully planned. Terrorists' tactics and targets, as well as the weapons they favour are unavoidably shaped by the group's ideology, its internal organisational dynamics and some times influenced by the personalities of its key members[6]. Terrorists act either nationally or internationally, especially after the development of telecommunication and transportation. There are terrorist groups who act only within their national borders, in a sense that they launch their attacks either against national targets or against foreign targets but in their national territory[7]. There are also others who launch their attacks outside their base, aiming either to hit an external enemy or to influence international politics or diplomatic relationships. Aeroplane hijacking and bomb attacks are the most usual examples of overseas terrorist action. Overseas action may be designated on a certain area, like the IRA[8] whose attacks target the United Kingdom, or on a certain country's nationals, like most Middle East terrorist groups who target mainly USA or Israeli nationals irrespective of the territory. Of course not all terrorist groups follow a certain pattern, but they all usually have discernible preferences that characterise their action.

b. The use of information technology.

Information technology, as already said, can be useful for terrorist groups in two ways: first of all,

computers and the internet can be used as a useful tool to enhance traditional activity and second, information infrastructure can constitute a new attractive target for terrorist actions. It has to be pointed out that although these are two separate issues, they have a strong interdependence. The fact that terrorists may use information technology as a useful tool does not automatically mean that information infrastructure will constitute their next target, extended use and familiarisation with technology, however, is a necessary step before deciding to turn against such targets. As they learn to use information technology for decision-making and other organisational purposes, they will be more likely to use it as an offensive weapon to destroy or disrupt[9].

The internet can be used by terrorists in various ways. First of all, it is very useful as a communication medium; electronic mail has become one of the quickest, cheapest and most effective ways of contacting between any part of the world. Furthermore, technology allows anonymous and secure communications and quick transfer of data, so terrorists can use the internet, at least theoretically, to exchange useful information on possible targets, like maps or instructions, and co-ordinate their action overcoming the obstacle of crossing national borders. Apart from that, internet is also an area where general information for potential targets or weapons are scattered[10], it can be a useful resource on its own. 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[11]. Terrorists are also said to use the internet to obtain funds, like several groups of Latin America and the Middle East[12]. Generally, computers can be as useful for terrorists as they are for law abiding individuals as storage media or as multipurpose "machines". According to reporters who visited Osama bin Laden's headquarters, the group possesses computers, communications equipment and a large number of disks for data storage. Hamas is another major group that uses advanced information technology[13]. These groups are also said to use strong encryption for secure communications and exchange of vital information[14].

The second way in which information technology can be useful for terrorists is by constituting their target. The growing dependence of our societies on information technology means that well organised attacks to vital networks can cause incalculable damage to public or private organisations [15], and, depending on how crucial is the system, entail serious injure or damage and inflict fear to civilian population. It is true that dependence on information technology creates a new form of vulnerability that did not exist before and it gives terrorists the chance to approach targets that would otherwise only be a wild dream, like the manipulation of a national defence system or an air traffic control system. It is however interesting to note that this vulnerability is not the same for every country, but it is analogous to technological development. The more technologically developed a country is, the more vulnerable it becomes to attacks against its infrastructure[16]. United States, even though extremely powerful, becomes the most vulnerable country in information technology attacks. The number of computers now installed in the US is estimated nearly 180 million, at least five times as many as in Japan, seven times as many as in Germany, and nearly twice as many as in all Europe combined. US computers account for 42 percent of the world's computing power, while China's represent 1 percent and Russia's 8 percent. Furthermore, even though the internet now expands across the globe, roughly 60 percent of its assets are concentrated in the US[17]. As for developing countries and the third world, information technology is gradually becoming all the more important, but not yet in a degree of dependence. So the problem has a different perspective there.

There are reasons to believe that terrorist groups have the ability and the means to make extended use of technology, either as a tool or as a target. As stated above, one of the most essential features of terrorism is its strong dependence on ideology; motivation is usually strong political or religious beliefs. This entails two things: membership in terrorist groups can be, first of all, independent of social or economic status, and, secondly, irrelevant to educational or intellectual background and potential. It is very likely that terrorist groups will make increasing use of information technology given the fact that some of their members are usually well-educated individuals comfortable with the use of technology. Additionally, they have ensured financial recourses, which means they have the

means to acquire technology and "employ", if necessary, the appropriate people to use it. The use is likely to rise as terrorist groups recruit younger members that are more familiar with technology. Furthermore, they are known to keep track of technological developments because the success of their actions partly depends on their ability to keep one step ahead of the authorities and of counter-terrorist technology. Probably they would use any means available to enhance their activity.

But the transition from traditional terrorism to the use of information technology, at least as a lethal weapon, is also dependent on two other factors[18]. First, they must understand and trust the use of the weapon. Terrorists seem to trust more easily weapons that they've built themselves or that at least have been tried by others, they usually do not seem very willing to experiment. They have to be sure that it will work. Most of the known terrorist groups seem to have certain preferences on the weapons they use and seem to follow a pattern on the attacks they launch. Second, it is also a matter of mentality; terrorists have to feel that a weapon is right for them before they use it, that it suits their ideology. A considerable number of terrorist groups seem to still like the feel of physical weapons. These are not, of course, the only decisive factors for the use of information technology and they certainly have nothing to do with using technology as a helpful tool for everyday activities. It is, however, important to keep in mind the special characteristics that differentiate terrorism from traditional crime.

An overall assessment would suggest that terrorists are technologically innovative but with certain limits. Although radical in their politics, the vast majority of terrorist organisations appear to be conservative in their operations. For example, while they were more active and considerably more lethal during the 80's compared to the 70's, the weapons they chose and the tactics they employed remained remarkably consistent[19]. It is not surprising that bombing is one of their favourites: it provides a dramatic, yet fairly easy and often risk-free means of drawing attention to the terrorists and their causes, few skills are required to manufacture a crude bomb, surreptitiously plant it, and be miles away when it explodes[20]. Consequently, although it is almost certain that terrorists will make extended use of information technology as a tool, it is still debatable if they will use it as a weapon aiming at information infrastructure as a new target.

The fact that information technology is widely available and is indeed being used by terrorists initially suggests that there is a call for special governmental action, aiming to eliminate the risks stemming from terrorists taking full advantage of it and enhancing their activity. But that is the exact point where one should be careful. Terrorism has traditionally provoked such intense concerns that there has always been a temptation to be careless in choosing the weapons to fight it. The fear that it 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[21]. More government secrecy, more police powers to detain people at will, less governmental accountability, less freedom and less privacy are not novel responses to terrorism[22]. It is important to assess the real threat posed by terrorist groups using information technology, keeping in mind that cyber-terrorism is not a term encompassing any use of information technology by terrorists. Governmental action against it could easily go beyond acceptable limits.

III. The phenomenon of cyber-terrorism

a. What is and what is not cyber-terrorism.

Even though terrorists seem to become more and more familiar with computers and the internet, it is important to clear out that not any malicious use of information technology constitutes cyber-terrorism. Cyber-terrorism is quite a new term, used to describe the convergence of terrorism and cyberspace. It is generally understood to mean attacks and threats of attack against computers, networks and the information stored therein, when done to intimidate or coerce a government or people in furtherance of political or social objectives[23]. However, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to

generate fear. Attacks that disrupt nonessential services or are mainly a costly nuisance would not constitute cyber-terrorism. For example, accessing remotely an air or road traffic control system and causing an accident resulting in loss of life or at least serious damage and spread of panic would constitute cyber-terrorism, while unauthorised penetration in a system aiming to distract information or simply disturb its users would not.

As there is not yet a clear idea on what exactly constitutes cyber-terrorism, there is a usual misunderstanding. The term is considered by many to cover many cases of computer and internet abuse, like hacking or the dissemination of computer viruses, and generally almost any incident of an on-line based attack whose only result is nuisance and, some times, economic loss[24]. It should be clarified, however, that the usual scope of these attacks is more for the perpetrators to test their abilities and prove to themselves and their targets that they can do it than to cause damage and inflict fear in furtherance of an ideology. There have been incidents, of course, that such techniques have been indeed used by terrorists but none of them has yet resulted in great damage, apart from financial. There is a new form of "disturbing" behaviour resulting from the wide abuse of information technology, but it should not be confused with cyber-terrorism. The criteria for an attack to qualify as cyber-terrorism, apart from the use of information technology, are also the identity of the persons who launch it, the scope for which they do it and the result. It would be quite authoritative to consider all these bothersome attacks as cyber-terrorism, because this would automatically vest them with all the special features that the term entails, and that is certainly not the case.

Cyber-terrorism should also be differentiated from the so-called "information warfare", the manipulation of computers and networks in the context of a war conflict between countries.[25] The latter is rather an offensive and defensive function of states, while the former is an intimidating tactics of non-state factors fighting for an ideology. These two may resort to the same techniques, for example the distortion of an electricity network, but still this does not make them the same phenomenon.

Cyber-terrorism should also be distinguished from "hacktivism", the term used to describe the convergence of hacking and activism. This term covers operations that use hacking techniques to disrupt normal function of systems, without causing serious damage, aiming at the dissemination of propaganda and expression of political opinions. Terrorists may resort to such actions in an effort to reach public opinion and make their ideas and beliefs widely known, or simply to annoy their opponents and make their existence known. That use of information technology works in the same context as using the internet to collect information about targets or to communicate and co-ordinate action with fellow conspirators or recruit supporters. Neither constitutes a complete terrorist action to qualify as cyber-terrorism. They are only an indication that, like with any other advance in technology, information technology is simply used to further unlawful purposes[26].

Cyber-terrorism then is neither a term encompassing all actual and possible uses of information technology by terrorists, nor any disturbing abuse of computers and the internet. It is the premeditated, ideologically motivated attack against information, computer systems, computer programs, and data which result in violence and serious damage against non-combatant targets, perpetrated by persons acting in the name of an ideology with the intention to spread fear and impose their existence to the public. The pure form of cyber-terrorism is the use of high technology tools against high technology targets[27].

b. Assessing the threat posed by cyber-terrorism and the general use of information technology by terrorists.

Assessing the threat posed to society from pure cyber-terrorism on one hand and the general use of information technology by terrorist groups on the other are two separate issues. Both are, however, essential to examine. Deciding whether there is a need for special action will not only depend on the

nature of the threat posed by pure cyber-terrorism but also on whether there is an unprecedented boost of terrorist action resulting from the use of information technology.

As for the first level of assessment, attacking vital information infrastructure could be very attractive for terrorists for several reasons. First of all, given the potential provided by computers and the internet, cyber-attacks to vital systems can be conducted remotely, anonymously and fairly cheaply, without requiring the handling of explosives or a suicide mission, which is usually a suspending factor when planning an attack. The dependence on information infrastructure gives an unprecedented opportunity for terrorists to aim at targets that would otherwise be extremely difficult to handle, and certainly impossible to be remotely disturbed, like air or road traffic control systems or energy distribution networks. Additionally, a successful attack resulting in enough damage to generate fear is certain to gain extended media coverage, which is a major priority for terrorist actions as it promotes public intimidation. Even though most hacking attacks are kept secret from the public to avoid spread of panic and loss of confidence on the compromised systems, a successful cyber-terrorist attack could not be easily kept away from publicity. Finally, information technology can work as a force multiplier because it allows attacking even the most crucial systems, for example defence and military networks that are certainly very attractive targets for terrorists but were almost impossible to influence before[28]. A survey conducted by the National Security Agency in 1997 revealed that the military operational systems in the US are vulnerable to unwanted intruders, that some times even go unnoticed. It has been estimated that defence systems in the US are being attacked by unauthorised intruders more than 250.000 times a year. Although no damage has yet been caused by these intrusions, at least not one that reached the public, the number is big enough to reveal vulnerability.

However, still theoretically speaking, there are also drawbacks for terrorists in exploiting information infrastructure. Even though vulnerable, systems are usually complex. This means that it might be difficult to control an attack and achieve a desirable level of damage or harm. Unless people are injured, there is less emotional appeal and a terrorist attack is less successful. Apart from that, it is probable that terrorists could be disinclined to try new methods and use new tools, unless they consider their old ones inadequate. As already said, terrorists need to be comfortable with a weapon before they use it and they have to feel that it suits them. Cyber-attacks entail remote handling which gives a feeling of insecurity and a difficulty in checking the actual result. Generally, terrorists do not have the tendency to experiment with anything available if they are not absolutely sure it will have the awaited result. Finally, we should not underestimate the human factor. Vital systems may depend on information technology, but there is still enough human control to prevent malfunction and cope with emergent and unexpected incidents[29].

Moving towards the second level of assessment, that is evaluating the actual use of information technology as a helpful tool by terrorists, one can draw an initial assumption. We have already seen that terrorist groups are indeed using information technology, but the situation is not much different than with the use of other forms of technology. It is utopian to believe that terrorists or any other criminals will not use the technological advances to further their ends. It is, however, very difficult to decide whether there is a direct connection between the use of information technology and the reinforcement of terrorist groups, at least in a level that would call for extended governmental action to eliminate it. In 1870 Nobel's invention of dynamite gave a new powerful weapon to terrorists, yet nobody has blamed Nobel for the rise of modern terrorism, nor has considered it essential to track any use of dynamite[30]. Terrorists have always used the means developed by states for legitimate purposes, this is unavoidable.

Last but certainly not least, apart from arguing on a theoretical level, we should also focus on available data. As for the general use of information technology by terrorists, it has already been said that terrorists do use information technology as a communications medium, as a means to recruit supporters, collect information, disseminate propaganda and raise funds to support their activity. However, it is difficult to collect absolutely reliable and realistic data. Terrorist groups tend to act

extremely cautiously, so it is highly unlikely that they will use technology, such as e-mail for example, in an identifiable manner. Furthermore, we still do not know the level of their ability to use information technology. It is highly probable that even if a successful attack to a vital system not aiming to cause great damage but only to warn for future actions, as for example a military defence system, had already happened, it would preferably have been kept secret so as to avoid embarrassment and loss of trust.

As for pure cyber-terrorist attacks, up to present there have been few, if any, computer network attacks that meet the criteria for cyber-terrorism. Most of the attacks that can be attributed to terrorist groups were launched merely to annoy or intimidate their targets, no great damages have occurred and no lives have been lost. In 1998, ethnic Tamil guerrillas swamped Sri-Lankan embassies with e-mail bombing. This incident, although characterised by US intelligence authorities as the first cyber-terrorist attack, did not result in any big damage. Since then, such techniques have been used during the Kossovo conflict in 1999, and they are a usual incident between parties in many conflicts around the world, such as Israel and Palestine, China and Taiwan, India and Pakistan[31]. These incidents, however, although usually perpetrated by small groups that could be characterised as terrorist, are more a phenomenon of cyber-war than pure cyber-terrorist attacks. A research conducted last year revealed that 90% of all intrusive activity on the internet is perpetrated by amateurs, 9.9% by professional hackers or corporate spies and only 0.1% by world-class cyber-criminals[32]. Another report[33] conducted last year, availing the changing threat of international terrorism, concluded that although the terrorist's toolbox has changed with the advent of the information age, the objectives of the world's terrorist organisations remain the same. The report stated that terrorist are adopting information technology as an indispensable command-and-control tool, but there is still no indication of whether information infrastructure will constitute their new target[34].

It is difficult to assess potential harm because we do not know how vital systems would react and we cannot foresee all ossible forms of attack. Whatever the measures taken, a risk still remains. Terrorists will always be a little ahead of counter-terrorism technology curve, because they spot vulnerabilities and launch their attacks, always well organised and planned, against them[35].

IV. Conclusions - Is there a need for governmental action?

The preceded analysis has shown that, although terrorists seem to be taking full advantage of information technology as a useful tool, there is no clear picture as to whether information infrastructure will constitute a new target. To date there are no incidents of pure cyber-terrorist attacks. That does not mean, of course, that no measures should be taken by governments. It is preferable to prevent such attacks than confront them when they actually happen.

However, clearing up the picture of what is and what is not cyber-terrorism and the actual threat it poses is important because it will be a decisive factor when choosing the weapons to fight it. The bad reputation of terrorism can be easily used as an excuse for extended intervention in the newly formed cyberspace. The fear intimidated to people by scenarios of potential harm can be manipulated to impose measures that otherwise would not be publicly accepted. For example, the fact that terrorists can use encryption to communicate is not a reason to abolish private communications *per se*. Information technology is as helpful for terrorists as it is for law abiding citizens, reaction to its malicious use should respect the assumptions of privacy and freedom that people legitimately expect.

The facts indicate that fear of cyber-terrorism is, at present, greater than the actual threat posed to society. In order to alleviate this fear and eliminate the possibilities of an actual cyber-terrorism attack governments should focus on security, and the key is clever security. By clever security is meant realising the importance of human factor. Instead of legalising methods of on-line investigation that considerably undermine privacy and other basic freedoms, governments should make sure that there is enough human control in all vital systems so as to prevent misuse by intruders with terrorist intentions. Prevention and not prosecution of cyber-terrorism should be the target.

Bibliography

(1) Arquilla, John and Ronfeldt, David , *"The Advent of Netwar"*, RAND Report for the Office of the Secretary of Defence, CA, USA 1996.

(2) Borland, John, *"Analysing the Threat of Cyberterrorism"*, (interview with W. Church, founder of the Centre for Infrastructural Warfare Studies) at <http://www.infowar.com/class_3/class_3102898b_j.shtml>.

(3) Denning, Dorothy E., *"Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy*", Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, at <http://www.nautilus.org/info-policy/workshop/papers/ denning.html>.

(4) Denning, Dorothy E., *"Cyberterrorism -Testimony before the Special Oversight Panel on Terrorism"*, Committee on Armed Services, US House of Representatives, 23 May 2000, at <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

(5) Devost, M., Houghton, B.K. and Pollard, Neal A., *"Information Terrorism: Can you trust your toaster?"*, at <http://www.terrorism.com/documents/suntzu.pdf>.

(6) Harmon, Christopher C., *Terrorism Today*, Frank Cass: London - Portland, Or, 2000.

(7) Hershman, Tania, *"Israel's Seminar on Cyberwar"*, 10/01/2001 InfoSec News at <http://www.securityfocus.com/frames/?content=/templates/ archive.pike%3Flist%3D12%26mid%3D155550>.

(8) Kelley, Kack, *"Terror groups hide behind encryption"*, in 06/02/2001 USA Today at <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm>.

(9) Kopel, David B. (Testimony) *"Hearings on Wiretapping and other Terrorism Proposals"*, Cato Institute - Committee on the Judiciary US Senate, 24 May 1995, at <http://www.cato.org/testimony/ct5-24-5.html>.

(10) Lesser, I. O., Hoffman, B., Arquilla, J., Ronfeldt, D. F., Zanini, M. and Jenkins, B. M., *"Countering the New Terrorism"*, Rand Report 1999, at <http://www.rand.org/publications/MR/MR989/MR989.pdf/>.

(11) Maher, Marcus, *"International Protection of US Law Enforcement Interests in Cryptography"*, 5 Richmond Journal of Law and Technology 13, (Spring 1999) at <http://www.richmond.edu/jolt/v5i3/maher.html>

(12) Pollitt, Mark M., *"Cyberterrorism - Fact or Fancy?"*, at <http://www.cs.georgetown/edu/~denning/infosec/pollitt.html>.

(13) Regan, Tom, *"When Terrorists Turn to the Internet"*, 7/4/1999 Infowar.com, at <http://www.infowar.com/class_3/99/class3_070499a_j.shtml>.

(14) Stark, Rod, *Cyber Terrorism: Rethinking New Technology*, at <http://www.infowar.com/MIL_C4I/stark/ Cyber_Terrorism_Rethinking_New_Technology1.html>.

(15) Verton, Dan, *"Terrorists use new tools, old tactics"*, 26/06/2000 Federal Computer Week, at <http://www.securityfocus.com/templates/ headline.html?id=7408>.

(16) Whine, Michael, *"Cyberspace - A new medium for Communication, Command and Control by Extremists"*, April 1999, at <http://www.ict.org.il/articles/cyberspace.htm>.

(17) White, Jonathan R., *Terrorism: An Introduction*, (second edition) Belmont, CA; London: West/Wadsworth, 1998.

(18) Wilkinson, Paul(editor), *Technology and Terrorism*, London: Frank Class, 1993.

(19) "Cyberterrorism: Overview of the Problem", at <http://www.mvhsmun.org/com/terrorism/internet.html>.

(20) "Statics on Cyber-terrorism", at <http://www.-cs.etsu-tn.edu/ gotterbarn/stdntppr/stats.htm>.

(21) Report of the National Commission on Terrorism, *"Countering the Changing Threat of International Terrorism"*, available at <http://www.fas.org/irp/threat/commission.html>.

---

[1] See Mark M. Pollitt, *Cyberterrorism - Fact or Fancy?*, at <http://www.cs.georgetown/edu/~denning/infosec/pollitt.html>.

[2] Jonathan R. White, *Terrorism: An Introduction*, (second edition) Belmont, CA; London: West/Wadsworth, 1998, at p.5.

[3] The term was initially used after the French Revolution in 1789, although with a different meaning: it used to describe a certain way of governance. Terrorism has taken many forms through history, it has evolved as it is now mainly after World War II, and especially after the 60's. See Bruce Hoffman, *Inside Terrorism*, London: Indigo, 1999.

[4] See Jonathan R. White, supra note 2, at chapter 1.

[5] See Christopher C. Harmon, *Terrorism Today*, Frank Cass: London - Portland, Or, 2000, pp. 4-10.

[6] See Bruce Hoffman, supra note 3, pp. 132, 154-158.

[7] ETA (Basque Fatherland and Liberty) for example, the famous Basque terrorist group, acts only within the borders of Spain and always against Spanish nationals, while 17 November (Revolutionary Organisation 17 November), the most famous Greek terrorist group, acts within its territory but usually against foreign targets, such as overseas diplomats or embassies.

[8] The Irish Republican Army.

[9] See I. O. Lesser, B. Hoffman, J. Arquilla, D. F. Ronfeldt, M. Zanini, B. M. Jenkins, *Countering the New Terrorism*, Rand Report 1999, chapter 3, at <http://www.rand.org/publications/MR/MR989/MR989.pdf/>.

[10] For example instructions on how to manufacture a bomb

[11] See Tom Regan, *When Terrorists Turn to the Internet*, 7/4/1999 Infowar.com, at <http://www.infowar.com/class_3/99/class3_070499a_j.shtml>.

[12] The Mexico's Zapatista Rebels, Peru's Shining Path and Tupac Amaru groups, the Revolutionary forces of Colombia, and also the Hezbollah, Hamas and Hizb ut-Tahrir in the Middle

East are using the internet for fund-raising. See *Cyberterrorism: Overview of the Problem*, at <http://www.mvhsmun.org/com/terrorism/internet.html>.

[13] See I. O. Lesser, B. Hoffman, J. Arquilla, D. F. Ronfeldt, M. Zanini, B. M. Jenkins, supra, note 9, at p.65.

[14] See Kack Kelley, *Terror groups hide behind encryption*, in 06/02/2001 USA Today at <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm>.

[15] See Marcus Maher, *International Protection of US Law Enforcement Interests in Cryptography*, 5 Richmond Journal of Law and Technology 13, (Spring 1999), p. 17, at <http://www.richmond.edu/jolt/v5i3/maher.html>

[16] See Rod Stark, *Cyber Terrorism: Rethinking New Technology*, (chapter one), at <http://www.infowar.com/MIL_C4I/stark/Cyber_Terrorism_Rethinking_New_Technology1.

[17] ibid.

[18] See John Borland, *Analysing the Threat of Cyberterrorism*, (interview with W. Church, founder of the Centre for Infrastructural Warfare Studies) at <http://www.infowar.com/class_3/class_3102898b_j.shtml>.

[19] See Paul Wilkinson (editor), *Technology and Terrorism*, London: Frank Class, 1993.

[20] ibid., p.13.

[21] See Testimony of David B. Kopel, *Hearings on Wiretapping and other Terrorism Proposals*, Cato Institute - Committee on the Judiciary US Senate, 24 May 1995, at <http://www.cato.org/testimony/ct5-24-5.html>.

[22] In UK for example the Prevention of Terrorism Act, giving unprecedented investigative and prosecuting power to law enforcement, has caused serious harm to human rights and has hardly immunised Britain from terrorism. See Testimony of D. B. Kopel (ibid.).

[23] See Dorothy E. Denning, *Cyberterrorism* -Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, 23 May 2000, at <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

[24] It is not implied here that financial losses are not important, however, they do not usually constitute the sole target of a terrorist action as they do not inflict the same fear as material damage or, even more, human injury. Terrorists may of course resort to such activity in order to annoy their target and maybe steal money, but this is not a pure form of cyber-terrorism. It is rather a simple incident of criminal activity on the internet.

[25] This phenomenon is also referred to by other terms such as "infowar" or "netwar". It is "the use of information and communications technology to influence, modify, disrupt or damage a nation state, its institutions or population by influencing the media or by subversion" as described by John Arquilla and David Ronfeldt, in *The Advent of Netwar*, RAND Report for the Office of the Secretary of Defence, CA, USA 1996.

[26] See Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy*, Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop, at <http://www.nautilus.org/info-

policy/workshop/papers/denning.html>.

[27] See M. Devost, B.K. Houghton and Neal A. Pollard, *Information Terrorism: Can you trust your toaster?*, at <http://www.terrorism.com/documents/suntzu.pdf>.

[28] See Michael Whine, *Cyberspace - A new medium for Communication, Command and Control by Extremists*, April 1999, at <http://www.ict.org.il/articles/cyberspace.htm>.

[29] See Dorothy E. Denning, supra, note 26, at p.15.

[30] See Paul Wilkinson, supra, note 19.

[31] See Tania Hershman, *Israel's Seminar on Cyberwar*, 10/01/2001 InfoSec News at <http://www.securityfocus.com/frames/?content=/templates/archive.pike%3Flist%3D12%26mid%3D155550>.

[32] Source: IBM Global Security Analysis Lab, Yorktown Heights, N.Y. See *Statics on Cyber-terrorism*, at <http://www.-cs.etsu-tn.edu/gotterbarn/stdntppr/stats.htm>.

[33] Report of the National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, available at <http://www.fas.org/irp/threat/commission.html>.

[34] See Dan Verton, *Terrorists use new tools, old tactics*, 26/06/2000 Federal Computer Week, at <http://www.securityfocus.com/templates/headline.html?id=7408>.

[35] See M. Devost, B.K. Houghton and Neal A. Pollard, supra, note 27.