Phd. Mirgen Prençe:
Lawyer; Lector in law at "European University of Tirana"
Cel: +355686070014/ **prencemm@yahoo.com**
Aldo Shkëmbi:
Lawyer; Lector; and PhD student in law at "European University of Tirana"
Cel: +355696699753/ **aldo-sh86@hotmail.com**

CYBER-TERRORISM IN THE AGE OF HIGH TECHNOLOGY

Abstarct

Over the past several years, terrorism has been one of the complex issues faced by government policy makers, analysts, and the public. The complexity of terrorism has emerged not only from the definition of the concept itself but also the tactics that terrorist groups use, the countries that support terrorist groups, and the policies and procedures that have been used to counter terrorist actions by the target countries.

In this perspective the concept of Cyber-terrorism present new challenges for law enforcement and policy makers. Due to its transnational nature, a real and sound response to such a threat requires international cooperation involving participation of all concerned parties in the international community. However, vulnerability emerges from increased reliance on technology, lack of legal measures, and lack of cooperation at the national and international level represents real obstacle toward effective response to these threats. Terrorists and cyber criminals will exploit vulnerabilities, including technical, legal, political, and cultural. Such a broad range of vulnerabilities can be dealt with by comprehensive cooperation which requires efforts both at the national and international level. "Vulnerability-Comprehensive Cooperation-Freedom Scale" identified variables that constructed the scale based on the expert opinions. Also, the study presented typology of cyber-terrorism, which involves three general classifications of cyber-terrorism; Disruptive and destructive information attacks, Facilitation of technology to support the ideology, and Communication, Fund raising, Recruitment. Such a typology is expected to help those who are in a position of decision-making and investigating activities as well as academicians in the area of terrorism.

1. Introduction

There is no doubt, the internet is becoming more and more of a major showplace for many people‘s lives. It is uncommon to hear that working or private life is not imaginable without it. When the first new computer was built in 1969 and later when the World Wide Web was created in 1971, the digital era began and the Internet soon became more and more present in all areas. The huge progress of modern media and technical possibilities opened up new ways and enabled us to interact fast.

However, the world does not always smell of roses and in times of international terrorism, the internet can easily be misused for cyber-terrorism. In the information age, cyber-terrorism has become increasingly dangerous and likely in the age of high technological transfers through the use of the internet and online databases. It has evolved into an attack on databases and security systems of nations, companies and crucial organizations. Dissidents are now able to hack into nations’ security information, electrical power and even gain control of weapons and military vehicles without being traced. Cyber terrorists also have the ability to target nuclear facilities and cause disasters. These attacks can wreck havoc and cause damages amounting to billions of dollars.

The present-day problem of international and national terrorism issues a challenge to society, authority, and peace services all over the world. Terrorism so far has claimed the lives of thousands and caused fear and instability. A long-term solution to put an end to this is not in sight despite the terrorist groups being well equipped, trained, and motivated. Irrespectively of the individual opinion and graduation of the issues regarding the internet security mentioned above, one has to notice that terrorism has already reached the internet for propaganda, recruitment, and other communications. It has also become a way to directly commit their offenses. Terrorists, in many cases, use the internet for strategic and practical purposes. They use it professionally and are also also highly aware of its weak spots as well. Besides this major aspect, some other points like the anonymity in the case of a cyber attack, regarding this issue and the abuse of young people‘s ability to commit cyber-terrorism, make this topic crucial and essential to our conference. In extreme situations, the information gained by acts of cyber-terrorism could be used to disrupt a state's security or even world peace. For example: a terrorist hacker acquires the atomic codes of a country with atomic power and displays this information

on the internet, or sells it to a possible buyer; the consequence would result in a world wide security threat, or a possible war. As one can quickly infer, it is in the interest of humanity to find a rapid and adequate solution for the topic at hand.

There is no current international agreement on the definition of cyber-terrorism and there have been disputes over whether the recent examples could be counted as cyber-terrorism. As the world becomes more reliant on technology, the world will have to work together to handle cyber-terrorism. The growing ubiquity of computers and their associated networks is propelling the world into the information age. Computers may revolutionize terrorism in the same manner that they have revolutionized everyday life.

Terrorism in the information age will consist of: conventional terrorism, in which classic weapons (explosives, guns, etc.) will be used to destroy property and kill victims in the physical world; techno-terrorism, in which classic weapons will be used to destroy infrastructure targets and cause a disruption in cyberspace; and cyber-terrorism, where new weapons (malicious software, electromagnetic and microwave weapons) will operate to destroy data in cyberspace to cause a disruption in the physical world. The advent of cyber-terrorism may force a shift in the definition of terrorism to include both disruption and violence in cyberspace in the same manner as physical destruction and violence. Through the use of new technology, terrorist groups may have fewer members, yet still have a global reach. The increasing power of computers may lower the threshold of state sponsorship to a point where poor states can become sponsors and rich states are no longer necessary for terrorist groups to carry out complex attacks.

2. Definition of Cybercrime

Cybercrime can be regarded as "computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks". In general, cybercrime can be defined as a crime committed in a cyber environment, including the Internet, computer networks, and wireless communication systems. In other words, cybercrime involves crime committed through use of the computer. This brings us to the issue of defining computer crime. According to typology of the crime committed using a computer, there are three types of computer-related crimes: a) A computer may be the "object" of a crime. This may involve theft of a computer software or hardware. b) A computer may the "subject" of a crime.

The computer in this category may be the subject for an attack. c) A computer may be an "instrument" to commit traditional crime.

3. Terrorism and Cyberspace

The terrorism is one of the most ubiquitous words in the current affairs, political or conflict news of the present day, few agree on exactly what is terrorism. As the famous cliché goes: *one man's terrorist is another man's freedom fighter*.

The understanding and perception of terrorism changed over the centuries. Terrorism was popularized during the French Revolution toward the end of the 18th Century with the régime de *la terreur*, which gave us the English word "terror". It had then a positive connotation as it was the system by which order was established during an anarchical period in France. Over time, however, its use became associated with anti-monarchy, anarchy, revolution, anti-establishment, violence and anti-government activity. The modern meaning of the word only emerged after the Second World War when terror was used to describe the anti-colonialistic, nationalistic and separatist revolts that were typically violent.

The five most frequently occurring ones were (1) violence and force; (2) political; (3) fear and terror emphasized; (4) threat; (5) (psychological) effects and (anticipated) reaction. The United Nations in the 1970s tried in vain to come to an agreement on what was and what was not terrorism. Many of its members held the view that struggles against occupation or oppression, or struggles for liberation, freedom or independence, even if they include acts of violence, should not be considered as terrorism In the light of the many events since the 1970s that involved all if not more than the five characteristics mentioned, the United Nations Office on Drugs and Crime (UNODC) has since adopted an academic consensus definition provided by Alex P. Schmid in 1988:

Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination – the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organizations), (imperiled) victims, and main targets are used to manipulate the main

target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought.

The term “terrorism” means any activity that involves an act which is dangerous to human life or potentially destructive of critical infrastructure or key resources, and which appears to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

There are probably as many motivations for terrorism as there are definitions. The three most common motivations are political, religious, and ideological. Of these, political motivation is the most prominent as it features in most definitions of terrorism. Grievances alone do not generate terrorist reactions, but they are more likely to occur if the discriminations are deemed to be unjust, and if violence is considered as a viable means to redress the situation. Regimes that suppress opportunities for political participation, either by denying access to power or by persecuting dissidents, are bound to create dissension. In such situations are the seeds for revolutionary terrorism sown. Terrorism is also likely to occur when the young élite find themselves at odds with society and its general passivity.

In the age of the high technology various terrorist groups have posted Web sites for specific purposes. Some like jehad.net and aloswa.org were set up by Al Qaeda, while others like 7hj.7hj.com, teach the use of hacking to serve Islam. The Hezbollah were known to operate three sites as at February 1998: hezbullah.org served as the central press office, moqawama.org described its attacks against Israel, and almanar.com.lb provided news and information.

The cyber terrorists are the newest and most dangerous group. Their primary motive is not just money but also a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems just to score their point. The threat of cyber-terrorism can be compared to those of nuclear, bacteriological or chemical weapon threats. This disheartening issue is that they have no state frontiers; can operate from any where in the world, and this makes it difficult for them to get caught.

However specific activities of terrorists include the use of the Internet for profiling, hiding identities, raising money, recruiting, information gathering, disrupting businesses, as well as for command and control, communications, propaganda and mobilization.

The value of the Web is so well acknowledged that almost every known terrorist group has a Web site. They cannot even be forced off, as they can either go to countries with broad free-speech laws, or take advantage of service providers who are unaware of their existence. For example, alneda.com was first hosted in Malaysia, subsequently in Texas and then Michigan, before being shut down in June 2002.

In spite of these setbacks, it is evident that electronic mail – encoded, encrypted or otherwise – is a critical component of communications for many terrorist groups.

4. Definition of Cyber-terrorism

Cyber-terrorism is basically defined as a deliberate, disruptive and threatening activity, with the intention to cause harm or further social, ideological, religious, political or similar objectives on government‘s computers and networks. This definition however is not determined or universally valid.

Cyber-terrorism can be considered as the convergence of terrorism and cyberspace, as the capability to realize basic hacks against individual systems using tools created by someone else, or as he capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. It is generally understood to mean 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. Cyber-terrorism also means the use of cyber-tools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population.

Further, 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 lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

To be more precise one have to think of cyber-terrorism more differentiated and from different points of view. If cyber-terrorism is treated similarly to conventional terrorism, then it would only include attacks that threaten property or lives, and can be defined as the leveraging of

target‘s computers and information, particularly via the Internet, to cause physical harm or endanger the infrastructure.

5. Types of Cyber-Terrorism

When talking about cyber terroristic attacks one categorizes these into the given categories:

Spyware: Non detectable worms that deduce information. Dangerous seeing as these worms are mostly undetectable and the victim does not know that he/she/ it is being attacked.

Vandalism: Web vandalism is defined by website defacement or denial of service attacks, initiated by a virus. This is dangerous seeing as these defaced websites can give out false information that is crucial to a certain cause or plans and can result in total change of policy.

Propaganda: Gathering information to influence the opinion of large numbers of people, which is a powerful recruitment tool for terror organizations. Dangerous since this can motivate hackers and gifted people to indulge in cyber-terrorism for a given cause.

Denial of Service: A virus that attempts to block and absorb the content of a certain resource to keep that resource from the intended user. This is dangerous seeing as this information might be crucial to an important, spontaneous decision that cannot be made without this source.

Network based attacks against civil or military infrastructure: As in conventional terrorism, critical infrastructure is an interesting target. However cyber-terrorism also deals with the penetration of fuel, water or electricity outlets. A virus is created that puts the control of fuel, water, or electricity outlets under ones direct command. This is dangerous because this can result in economic breakdown when dealing with infrastructure that has to do with banks, or stocks, leakage of chemicals, and in connection with chemical storages etc.

Non-Network based attacks against civil or military infrastructure: Equipment disruption can also occur from non-computerized attacks. An Electromagnetic Pulse (EMP) occurs after a nuclear device is detonated, and disables all electronic devices within range. Altering virus: A virus that alters commands inflicted upon software via the computer. Most dangerous when used to interfere in military command.

6. The Convention on Cybercrime and Cyber-Terrorism

As a threat, cyber-terrorism would probably not justify a convention to deal with it. The explicit inclusion of cyber-terrorism in the Convention on Cybercrime by means of an additional

protocol would probably suffice. Whatever the choice, it is, however to fight cyber-terrorism there is no need for a definition. The broad acceptance of the 1988 Rome Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation shows there is no need to use "scare words" in order to reach consensus. In fact, it was probably due to the lack of such words that the Rome Convention was so successfully adopted. Thus, given the fear of terrorism in our society, an Additional Protocol to the Convention – either detailing some offences that would be considered cyber-terrorism or specifying when the offences established in the Convention should be considered more than just cybercrimes – should be enough. The effectiveness of this Protocol, as well as of the Convention itself, would however depend on the number of States that ratify them.

7. Conclusions

The fact that cyber-attacks can come from anywhere in the world makes investigation, producing evidence and taking the offenders to court an immense task that can only be achieved through international cooperation. The Convention on Cybercrime was designed to help accomplish the goal of reducing and/or tearing down the difficulties of the fight against cybercrime. Still, it shows itself to be insufficient because international collaboration in not injunctive and there are no rules to unload the burden of formality from the work of police specialists in charge of investigating international cyber-terrorism cases. Furthermore, the fact that key Member States of the Council of Europe are taking their time to ratify the Convention also leaves a bitter notion of lack of interest in cybercrime, one type of crime that is becoming increasingly important for companies all over the world. Let's hope our countries don't wake up too late. It is easy to be wise after the event!

While there have been many studies in the separate areas of terrorism and cyber-terrorism, it is hoped that by putting them together we can establish the significance of the cyber-terrorism threat. We have verified that cyber terrorists are likely to have similar motivations with terrorists in desiring violence and destruction to meet their political or other causes. While there have been no clear acts of cyber-terrorism to date, this could be the result of lack of motivation or ability to carry out the attacks in cyberspace and not the feasibility. However, this situation is not expected to remain as is, given the advantages offered by cyber-terrorism against forces and societies that rely heavily on information technology.

But however if it is possible to deceive terrorists, then it should also be possible to deceive cyber-terrorists. The reliance of cyber-terrorists on information technology makes them vulnerable to cyber deceptions. In addition, many of the methods and tools that cyber-terrorists would use are similar to those used by other less malicious hackers, so we can plan specific deceptions to use against them in advance.

It is known that there is much literature available on the methods, motivations and psychology of terrorists, but little is available in comparison for cyber-terrorists. What is available tends to be confined to arguments on the nature of the threat, rather than the threat itself. Thus more work will need to be done on studying the vulnerability of critical information systems, their potential exposure to cyber-terrorists and the damage they could do if they gained access. Finally, just like updating an anti-virus software against new strains of viruses, cyber deception methods that are being developed need to be constantly updated to remain relevant in their ability to deceive a cyber-terrorist attack.

Biblografy

- Illena Armstrong. "*Real Risk or Shadow? The Threat of Cyberterrorism"*. Articles and Features, January 2003. http://www.scmagazine.com, accessed August 2003.
- Burgess M. "*A Brief History of Terrorism"*. The Center for Defense Information, July 2003. http://www.cdi.org/terrorism, accessed October 2003.
- C. Carr (Ed). "*The Book of War"*. New York: Random House. 2000.
- Crenshaw M. "*The Causes of Terrorism"*. Comparative Politics, pp381- 385. July 1981
- Martha Crenshaw. "*Terrorism in Context"*. Pennsylvania State University Press. 1995
- Dorothy E. Denning. "*Information Warfare and Security"*. New York: ACM Press 1999.
- Dorothy E. Denning. "*Cyber/terrorism!*. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, May 23, 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, accessed July 2003.
- Dorothy E, Denning. *Is Cyber Terror Next?* Georgetown University, November 2001. http://www.ssrc.org/sept11/essays/denning.htm, accessed July 2003

- James F. Dunnigan. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press Books, 2002.
- Hoffman, B. *Inside Terrorism*. Paperback Edition, London: Indigo 1999.
- The Honey Net Project. *Know your enemy*. Boston: Addison-Wesley, 2002.
- Rawles, James W. "*High Technology Terrorism*." *Defense Electronics,* January 1990, 74.
- Sitomer, Curtis J . "Crooks find Computers Useful; Terrorist see Vulnerable Targets."
- *Christian Science Monitor,* 5 December 1986, 6.
- Th,Thomas Perry, "*Terror as a Weapon of Political Agitation*," *Internal War: Problems and Approaches,* ed. Harry Eckstein (New York: Free Press of Glencoe, 1964), 73.
- E.F. Mickolus, *Transnational Terrorism: A Chronology ofEvents, 1968-1979*
- (London: Aldwych Press, 1980), XIII-XIV as quoted in Schmid *Political Terrorism.*
- R. Clutterbuck, "*Guerrillas and Terrorists"* (London: Faber and Faber, 1977), 11,21 as quoted in Schmid, "*Political Terrorism"*.