diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 23/05/2013

All'indirizzo http://www.diritto.it/docs/35076-computer-terrorism-as-a-new-form-of-terrorism-in-the-modern-society

Autore: Enver Buçaj

Computer terrorism as a new form of terrorism in the modern society

COMPUTER TERRORISM AS A NEW FORM OF TERRORISM IN THE MODERN SOCIETY

Enver Buçaj, PHD Cand.

I. Introduction

In the past twenty years ([1]) the computer smart users, have astonished the world through using their personal computers to commit crimes, consequently creating a strange feeling of admiration and fear amongst other users.

The entertainment industry has understood these emotions quickly and for this reason it has continuously published new books, movies and plays that represent cyber criminals in action, threatening the world from sitting behind their computers.

The dependence of the society today on the computer technology is enormous and is increasing every day. The digitalization of the working process in all social and economical spheres of life is a real phenomenon today and it is growing every day. The development of world trade has a direct effect on the further development of the computer technology and interne. This development of the industry has created an opportunity for the use of these computers to commit different cyber crimes and terrorism.

Studies that have been conducted on the topic have lead to the establishment of several definitions of the term 'computer terrorism'. The essential meaning usually attributed to computer terrorism is an etymology that originates from the ideas shaped initially on the sphere of computer technology and terrorism. Nevertheless, computer terrorism is an attack that aims at the disruption of the connection between the material world or the real world and the virtual one. In today's modern era it is obvious that there are similarities between the virtual world and the world we live in that the two of them are being integrated with one another. This tendency has lead to the creation of the many agencies and organizations for protection against computer terrorism. Hoverer, these institution have become targets to many computer terrorism attacks, due to the fact that the extinction of the functional anti-terrorism system would facilitate the achievement of the goals of these villains with less endeavors and expenses ([2]). These studies have also shown that computer terrorism is " a premeditated use of destructive activities, who's aims are social, ideological, religious, political or similar, and intend to frighten every person" with regards to the abovementioned objectives.

There is a need for awareness rising amongst the society regarding the notion of cyber terrorism and the possible threats that can result as a consequence of the use of the latest technology by the terrorists, a occurrence that is being expanded day by day.

---

[1] The author is a doctoral candidate at the University of Prishtina/Kosovo, working on the topic 'Preventing and combating cyber terrorism' and he is also affiliated with the University as a Lecturer. Has been a founding Academic Director of the second public university – the University of Prizren, where he is currently a lecturer. Among others: held the position as a Senior Adviser for Higher Education to the Minister of Education, Science and Technology in Kosovo; Manager of the Finnish Program for Human Rights in Kosovo. Speaks fluently the following language: Albanian, English, Finnish and Serbo-Croatian.

[2] C. BARRY. *Where the virtual and the real world touch*". 11th *International Yearly Symposium for Matters of Criminal Law*, IL: University of Chicago, 1996.

According to the Federal Bureau of Investigation (FBI) Computer terrorism is a premeditated attack conducted by secret agents or clandestine groups, motivated politically, targeting computer systems and programs, informational systems, military objectives and databases that contain information regarding these military objectives. Unlike a simple annoying virus, a cyber attack is designed to cause physical pain and to destroy the financial services. Computer terrorism is however the simple use of the computers and internet network to design and conduct terrorist attacks. It is an actual fact that now-days someone or certain groups might use computer and technological means to conduct a military or a terrorist attack against certain targets ([3]). Furthermore, the notion computer terrorism or the cyber crime refers to a crime that usually involves using a computer and a network and it has often been referred to as electronic terrorism or the 'war of information'.

The computer despite being used as a tool to conduct the crime can also be a target of the attack. Nevertheless, the notion computer terrorism usually refers to the criminal use of internet and the computers. Crimes like these can threaten the national health and security of an entire nation. These types of crimes are considered as crimes of a high profile especially the ones related to the outbursts regarding the author rights, children pornography and human trafficking. There are also many problems with privacy issues in cases when the confidentiality has been breached in different ways. Possible target objectives of the cyber terrorism attacks include: the banking industry, military stations, thermo centrals, centers for air traffic and water services, etc. [4]

It should be noted that there are two similar terms that one can encounter in the literature, 'computer terrorism' and 'cyber terrorism'. These question is, are these terms exact synonyms? The answer is no. I believe that despite what has been said so far these two terms describe a similar idea but expressed in different timings and circumstances. Cyber crimes although committed through the use of a computer are carried on in a different cultural and technological context of cybernetics than the computer crimes.

Computer terrorism is one of the most serious forms of crimes often compared to biological and chemical weapons, and viruses. Furthermore it is a crime that is really difficult to be tracked down to its source. There are no borders to what can be affected by this form of crime, and basically can attack all kinds of computers spread out equally all around the world. Tracking down and neutralizing this type of crime is a very difficult task due to the fact that there are usually not many traces left compared to the real life where the traces are more obvious and easier to track. Unlike the real life terrorists who use explosives or small weapons in order to reach their goals, computer terrorists use the modern technology and information systems, computer networks, specially designed and unauthorized software's to reach their goals.

II. Forms and characteristics of computer terrorism.

There are dozens of countries that have been targets of sporadic and destructive attacks from terrorism networks within their countries or those sponsored by other countries. As already stipulated above, unlike the classic forms of terrorism, the terrorist have started using new means of conducting their actions related to technology, victimization, threats and reactions.

The best example to describe the situation is the case of Ramsi Jusuf, the person who organized the attacks of September 11th 2001. By using the computer technology he received the messages and the instructions for organizing the actions and deciphered all the codes ([5]). 'Nine Eleven' is considered to be as one of the most destructive attacks registered in the past centuries. Eleven terrorists' high jacked

[3] http://searchsecurity.techtarget.com/definition/cyberterrorism
[4] US. Commission of Critical Infrastructure Protection
[5] A. YONAH, *Combating Terrorism, Strategies of ten countries*, University of Michigan 2002

four airplanes with passengers, two of which crashed on the Twin Towers namely the Center of World Trade in New York, one was aimed at the Pentagon in Virginia, and the last one crashed in a field in Schwenksville in Pennsylvania which was not a target. Consequently around 3000 people lost their lives and thousands were injured. The attack came as a surprise since something similar had never occurred before and this caused a lot of concerns regarding the national security of U.S. The fear continued to spread in the following years and there are still concerns that the 'nine eleven' attacks will be repeated in a greater extent and by different authors (i.e. states, organizations or individuals) that will try to reach their goals even by using the biological, chemical and atomic 'super-terrorism'.

These conventional and non-conventional challenges against the stability world wide require effective national, regional and global efforts in order to face all the forms of terrorism including the computer terrorism. During these kinds of terrorist attacks, the actions threatening the security are interconnected and similar to one another despite being conducted by different people. In this sort of scenario the computer technology has its advantages due to its efficiency on reaching the goal ([6]).

For a while now the analysts have stated that the new terrorism depends on the technologic and informative revolution. In reality, terrorism is interconnected with 'information' in so many ways starting from the fact that there has been a tendency to keep hidden from the international media the names of the people that are trained for actions of suicide bombing. Or in the other hand the attempt of the terrorists to occupy the front pages of the papers with their criminal actions, up to the media debates regarding the countermeasures that would limit the freedom of press, the increase of the public supervision and the data collection and the increase of the security of the systems of communication and information. The terrorists focus their tactics on the important information and communication such as the ones regarding the functionality of the democratic institutions, on the debate on how the terrorist threats underestimate the democratic practices that can be developed with regards to the issues of freedom and information technology ([7]).

It is obvious that international criminal groups can attack the data networks and structures of any state including the US by using relatively simple tools. Taking in consideration that these attacks are not difficult to plan there is a slight concern regarding possible threats in the future. As witnessed the means used are switching day by day from the classic ones such as the bomb machines - targeting a single communication or data center - to electronic means of attacking an entire network. These recent methods can include hiring different hackers to commit certain crimes. However it is more likely that the crimes be committed by certain terrorist groups that have capable people with them and that are able and have used the internet and other means to communicate with one another. The groups of interest include well known organizations with long term reputation such as the Lebanon Hezbollah , and other unknown international terrorist groups and less known organizations such as the ones responsible for the 'nine eleven attacks' to the World Trade Centre.

By using these new technologies, terrorists can undertake new attacks targeting the most essential information systems and economic databases. Due to this spread of the threats the international community has enacted several sectorial conventions against computer terrorism, and these conventions are open for ratification by all the states.

III. **The international character of computer terrorism as a criminal legal phenomenon.**

[6] P. FLEMMING – M. STOH, *Myths and Realities of Cyber terrorism*. 2001.

[7] J. ARQUILLA – D. RONFELDT – M. ZANINI, "Networks, Netwar and Information–Age Terrorism," In: Ian O. Lesser, Bruce Hoffman, John Arquilla, David F. Ronfeldt, Michele Zanini and Brian Michael Jenkins. *Countering the New Terrorism*. Santa Monica, Calif.:Rand and John Arquilla and David Ronfledt. 2001. "Networks, Netwars, and the Fight for the Future, "*First Monday*, 1999 volume 6, number 10.

According to a database that contains data regarding the international crimes, computer terrorism as a criminal legal phenomenon is characterized as international crime. Studies have shown that the use of internet is increasing day by day and with it increases the phenomenon of computer terrorism.

The Internet network today is spread almost through the entire world thanks to the use of new technologies -the use of the satellite mobile communication tools has enabled access to internet almost in every part of the world. More concretely the internet network covers more than 180 countries all around the world. Hence the expansion of the use of the computers and the modern technology has resulted in the new forms of crimes such as the computer crimes and terrorism, unauthorized access to the computer networks and systems, the massive breakings and thefts, illegal money transfers, etc.([8]).

According to the experts at the European Council, the amount of the stolen money only by the use of credit/debit cards every year amounts to approximately 400 million €. Different forms of viruses cause around 12 billion € losses every year, and approximately 250 billion € worth of property are embezzled every year ([9]). Furthermore, the computer terrorism is becoming a serious threat to the efficient function of the governmental institutions in the fulfillment of their obligations and applying the law. Moreover several criminal organizations use the internet as an easier way for recruitment of the younger generations.

Today's society is depending more and more on technology, the role of the virtual world in the daily realistic existence is increasing day by day and becoming an essential element to it. There are a lot of advantages to the use of computer technology at work, market and government, these advantages however are being threatened to use for purposes of committing different crimes all around the world through the simple use of a computer connected to a network. Former director of CIA, George Tenet, had declared that terrorist groups such as Hejsbulla, Hamas, Abu Nidal and one of the largest organizations led by Bin Laden – Al Qaeda, are very active and use the computer technology in their daily performances.

Therefore all governmental and non-governmental stakeholders must participate jointly in combating and preventing computer terrorism, espionage, online hacking of the financial systems and other types of cyber crime. The fact that the computer terrorism is often spread beyond borders is imposing a higher risk upon the governments of states hence it is often referred to as 'cyber warfare'. So far there have been several attempts to condemn the preemptors at the International Criminal Court.

Consequently it is very important to initially define terrorism under international criminal law. The international treaties require that all kinds of terrorist activities be prevented and convicted, but beforehand be defined. The strict definition of the crime within the text of these international treaties is significant in many ways. First and most important it is the symbolic and normative purpose, namely defining an abstract way the sentence for the criminal act committed. Secondly it eases the process of concluding international treaties. A clear definition of terrorism excludes the possibility for states to avoid their obligations due to the non-clarity of the provisions, hence the states are obliged to respect all of the obligations undertaken, no matter how strict those undertakings are, but at the same time it also limits the scope of these obligations relating them only to the definition and makes these agreements less costly. Third, it sets a very good ground for the fulfillment of the legal obligations and sets the ground for a better international cooperation in the police level. This efficiency and cooperation is particularly important in the cases of extradition, where most of the national legal systems require

[8] J. TRAVNIKOV, *Crimes in the Web: Borders without the deputies.*

[9] M. DELIO, *Inside Russia's Hacking Culture* [Wired News, March 12th 2001 http://www.wired.com/news/infostructure/0,1377,42346,00.html]

that the terrorists be convicted in the requiring country same a in the required country. And lastly, it is very useful in codifying the internal legislation regarding the criminal acts and the perpetrators, and punishing the criminal acts defined within the treaties in accordance with their human rights. The widely known principle 'nullumcrimen sine lege, nullapene sine lege' requires the states to define in detail the crimes for which a person can be prosecuted, so a person cannot be prosecuted for a crime that he has committed if at the given time the action was not included as a crime within the framework of the law.

IV. The harmonization of the legislation on prevention of the computer terrorism.

All countries are under the obligation to harmonize their national laws concerning he prohibition and prevention of the computer terrorism in accordance with the international law standards. In order to prevent the international terrorism states must act together as one and do so by designing and utilizing a joint database. On that regard the international community has approved a more sectorial standing and access with the aim of identifying all the violation acts conducted by the terrorists. Also the actions of the individuals conducted outside the framework of the treaties with the purpose of categorizing of these actions.

Basically, the conventions on the sectorial approach confirm the assumptions that several criminal acts can be treated as actions with international interest despite the aim of the terrorists or the target. The main advantage of this approach is the fact that it avoids the need to redefine the computer terrorism within the national level since it is already defined in an international level. So as long as the convention is in force there is no need for other definitions of the computer terrorism. A different particular definition would come handy in case the actions were committed under specific circumstances. However it would still be counter-productive given that it would result in an unfair treatment.

The goals of the actions of the computer terrorists are a description of the scope of the actions they can actually commit. The main types of actions or crimes the computer terrorists can commit include destroying various systems or networks and interrupting the broadcasting of various programs or information. The act of destruction can be undertaken in many different ways, namely through different types of viruses that can be installed or uploaded and affect the entire network. Another harm that can be caused by the cyber terrorists is changing the data in the important confidential databases that sometimes results in blocking access to that information for the competent authorities. It often occurs that the databases are breached with the purpose of re-transmission, particularly in cases where there is a certain interest in the data within the targeted databases. This is usually the case when the targeted databases are the confidential ones, such as the governmental databases ([10]).

One of the main elements that studies have focused on with regards to the threats that can come from the terrorists through the Internet is defining the possible ways of actions and behavior of these terrorists. Amongst the ways these plans can be attributed to terrorists is observing the entire network and the population. This can be done in different ways and from different distances, given that the network is used by so many consumers to transfer their data from a place to another in a very efficient time, and for any purpose. Another usual action conducted by the terrorists is using the network to detonate bombs that can be controlled from long distances and can be detonated simultaneously ([11]).

---

[10] A. SAVINO, *Cybernetic Crimes. 2001. University school of law: Cyber crimes. Available: http://www.cybercrimes.net/Terrorism/ct.html*

[11] Id.

There are several other scenarios of destructive terrorist attacks that can be undertaken that involve changing the formulas on the medications or the medical plants, exploding communication networks, mixing up the train schedules, changing the pressure in the gas tubes with the purpose of damaging the valves, destroying the functionality of the air control mechanisms, causing the explosion of the oil refineries, destroying the software programs that are used by the emergency services, electric cuts and detonating simultaneously hundreds of bombs all over the world ([12]).

V. The Cyber Warfare

The Balkans region is known for the many wars in history and it has recently been exposed to new forms of war, that of the cyber warfare through the use of technology. The cyber warfare has particularly been obvious between Kosovo and Serbia, since both parties have used the internet technology for the purpose of broadcasting the news from their own perspective.

However, some of the attacks sometimes focus directly on the parties involved. An example of that is the case of the officials in charge of maintaining the webpage of NATO, who were direct targets of an attack, when their emails were flooded with more than 2000 emails from Serbia within a day. Some of these emails included highly destructive viruses, which impaired the work of the NATO system for a while after ([13]). The main goal of the attack at hand was to damage the functionality of the NATO website by blocking it by the amount of emails, and to cut down the communication through the viruses. Fortunately the attack was only partially successful.

Although these sort of attacks result in a significant damage of very important information they are usually not qualified as computer terrorism. But the fact that these attacks have occurred before illustrates the fact that these kind of actions are easy to be undertaken and have been done before originating from small places.

With regards to the conflict between Kosovo and Serbia, it should be noted that despite the fact that the armed conflict has come to an end, the parties continue to have a conflict through the use of internet. On the 3rd of august 2011 the Serbian hackers breached the web page of the Parliament of Kosovo, and left an inscription stating "On protection of the Serbs in Kosovo". In addition while the web was under the attack of the Serbian hackers, the Serbian anthem was played on the background once the page opened. Furthermore, there were many links posted on the web connecting to web pages that contained propagandistic information against Kosovo and the Prime minister of the Republic of Kosovo. According to an online portal- Index Online, the website was down until 04 of August 2012 when the maintainers of the web managed to take control over it, and return it to the previous state ([14]).

On the other hand, on the 8th of July 2011, the Kosovar-Albanian hackers in sign of revenge for the situation in the North of Kosovo, breached into the website of the Serbian government. The attack carried on by the "Red and Black Hackers" targeted the web http://srbijabrend.gov.rs, and they put a map of the Ethnic Albania, with the slogan " Kosovo is Ilirida" and the message description as following: "We will not stop until you stop with all the offences against Albanians". They had also attached a file with national Albanian patriotic motivated music videos.

---

[12] A. YONAH, *Combating Terrorism, Strategies of ten countries.* University of Michigan 2002.
[13] British Broadcasting Corporation BBC, 1999
[14] http://www.kuvendikosoves.org/dhe www portaliIndeksonline.net 04.08.2011

The actions above are just a few examples, of less harmful actions that can be conducted through the use of internet. The computer terrorism attacks are known to cause more damages, and this dangerous occurrence is no longer a myth but an ugly reality. Moreover the latest technology developments and its wide spreading will lead to a more advanced types of attacks including the more dangerous ones such as the computer terrorism attacks ([15]).

Therefore it is considered that computer terrorism will become more and more attractive to the cyber terrorists ([16]). This is due to a number of factors, such as:

- The risk of getting caught after committing a crime has been reduced due to the possibility of undertaking an action from a long distance.
- It is possible to cause large amount of economic and technical damage without affecting the lives of people
- The experts on these issues can be easily hired for the job.
- A successful attack will make the front pages of all the media all around the world whilst the unsuccessful one will go unnoticed.
- The internet can be used as a tool to generate money all over the world.
- The internet offers great possibilities for spreading propaganda about a terrorist group that works on a global basis and that cannot be controlled by an individual government.
- The attacks can be prepared and conducted in a short amount of time and with little expenses.

The issue of the spreading of the computer crimes has been taken very seriously in the past few years by most of the countries of the world especially by the United States of America, where such concerns about the IT (Informative Technology) have lead to the establishment of the National Infrastructure Protection Centre (NIPC). The centre has employed a significant number of people (500 from all over the country) including representatives from all the existing agencies such as the Secret Service, CIA, NASA, National Security Agency, Department of Defense and others. The main goal of the centre (NIPC) is "investigating, discovering, evaluating, predicting and preventing, the possible computer and network breaches and illegal attacks" that threaten the centers or headquarters of the essential infrastructure in the US, for example, those of telecommunication, energy, banks and finances, water systems, government operations and other emergent systems ([17]).

According to sources from the CIA, China and Russia are amongst the states that use the computer systems and networks for espionage. In the recent documents published by the governments of these countries there are indications of the "Cold War" conducted in distance through the use of computer networks with the aim of obtaining illegal information. According to Robert Bryant, a high official at the CIA, this is an illegal activity and a direct threat to the American economy. However, in a press release the Chinese and Russian ambassadors in US have overruled the claims of the CIA officials.

In the CIA report it was stated that the internal networks of some US companies were under constant attacks from the 'Chinese hackers". Including the most clicked website in the world – Google, whose officials have admitted to have lost significant confidential data in 2011 as a result of a breach originating in China. These attacks have reached a high level of sophistication, consequently it requires

[15] Portal, Indeksonline , 2011, www.indeksonline.net
[16] Ibid
[16] National Insurance Protection Center, 1998
[17] W. G. KRUSE – J. G. HIESER, *Computer forensics: incident response essentials*. Addison-Wesley. Publisher, Boston Addison Wesley 2001

a high level of network of experts that is usually hard to be put together and organized outside the framework of the secret services of the governments ([18]).

In a computer guided crime world it is getting easier and easier for the criminals to avoid getting caught and punished for their actions, given that they act from place to place, and sometimes from places where such behavior is not considered a crime and the person cannot be persecuted for these actions. The authors of these actions might also be under the impression that the agencies for fighting computer crimes are located in a different country hence cannot persecute people in another country for such an attack. Mr. Kevin Di Gregory - general deputy-assistant in the Criminal Division of the US State Department at the European Parliament in 2000, gave a statement with regards to the above issues as following:

"Think about a hacker in Paris located in the left side of river Seine, on the other hand a company located in the right side of the river faces a crash in the system. Before the connection to the victim was interrupted the author of the action wrote to several bidders who were interested in the information in Rumania, Australia and Argentina and sold them the information. In this case the French police will need assistance from the authorities in Bucharest, Canberra, and Buenos Aires, before finding out that the action has originated in Paris ([19]).

On real life crimes, the boarders impose an obstacle for the perpetrators, since it would be difficult to commit a crime outside the national borders of their country. When it comes to computer crimes however, there are no borders for the authors of the criminal actions, but the agencies for law enforcement on the other hand are restricted by their territorial jurisdiction and they must respect the sovereignty of the other countries. As a result these agencies are required to cooperate with other foreign agencies on their mission of law enforcement and fighting computer terrorism. Unfortunately the differences in procedures and incompatibilities in law impose an obstacle on this cooperation between the agencies on their effort to prevent and fight the computer terrorism.

Failure of a country to condemn and punish the criminal actions related to the computer technology is an obstacle to the law enforcement. In cases when the laws of one country penalize certain actions conducted through the internet networks but the laws of another country do not than the international cooperation between these two countries might be impossible due to the differences in the legal system. Especially in cases when the criminals use more than two or three computers located in different places until it reaches the targeted destination. An incompatibility in only one of these places can cause trouble in prosecuting the author for the given crime.

VI. The globalization of computer terrorism.

The globalization of terrorism in the past decades consequently the increase on the consensus that these actions should be criminalized and not go unpunished has lead to strengthening of the international cooperation, especially in the past decade. This close international cooperation has required an intensive diplomacy by all the countries, and a close cooperation between the Ministries of Foreign Affairs and the agencies for preventing and punishing crime, and rule of law protection. There many signs that show this international cooperation, such as the recent resolution by the UN General Assembly that condemns the terrorism and requires all the states to cooperate in combating computer

[18] www. albeu.com
[19] K. DI GREGORY, *Fighting Cybercrime – What are the Challenges facing Europe ? The Transatlantic perspective*, U.S. department of Justice, September 19th 2000, http://www.cybercrime.gov/EUremarks.htm

terrorism. A similar decision was made by the International Islamic Organization in 1995. Other countries joined the trend by organizing several conferences against cyber terrorism, mainly sponsored by Philippines, Japan, Argentina, Peru, etc. ([20]).

A key element in achieving international cooperation in fighting the computer terrorism is harmonizing the laws amongst the states. However in reality there is still a long way to go until that happens, due to the hesitation of the countries to open up and let go a bit of their sovereignty. The indications are that such harmonization will not be happening in a near future, mainly because of the sensitivity of the field and the strong protection required. So far about 50 countries have harmonized their legislation, despite the fact that the process has started in 1950, right after the approval of the Universal Declaration of Human rights. Therefore there are a lot of difficulties on the process of the harmonization due to the nature of the crimes itself.

Consequently the computer terrorists can use the loopholes on the legislation and conduct the crimes from the places where these actions are not criminalized, and they cannot be persecuted for these actions. Hence in order to fight the international computer terrorism the internal national regulations are not sufficient, since that is only a partial solution of the problem.

VII. Conclusion.

As already stated above when the criminal action is undertaken in one country but targeting people or institutions in other countries than it becomes internationalized, and is referred to as international computer terrorism. Most of the countries in the world are interested in fighting this new form of terrorism be it national or international. In order to fight this terrorism high and intensive level cooperation amongst countries is required. This cooperation can only be achieved by creating an international worldwide network to fight the computer crime ([21]).

Therefore, the computer terrorism cannot be fought only through civic education, if there is no international cooperation in combating terrorism and harmonizing the national laws. Since this occurrence has taken the format of an international crime there is a need for creating international joint standards for protecting the computer network systems with the aim of preventing and combating computer terrorism. Without these joint international standards, the war against computer terrorists is quiet difficult given that most of the authors of these crimes are professionals.

The best suitable tool to fight this form of organized crime if through the enactment of new laws, in harmony with the international standards and by encouraging the cooperation and coordination amongst the national state agencies for enforcing these laws.

[20] A. YONAH ,*Combating Terrorism, Strategies of ten countries.*
[21] A. DEMOLLI, *Terrorism*, (p: 284-285)