# CYBER-TERRORISM AS A THREAT TO NATIONAL SECURITY

*Jasmin Kalac, p. 119-127

*September, 2017; 2 (2)*

## ABSTRACT

The tremendous achievements and the development of the leading technology, sophisticaled computer systems opened new “cyberspace” that constantly destroys the old traditional forms of organization, behavior and belief. Cyber information led to cyber revolution and the emergence of the information society, which dominates the race for information and communication technologies, in parallel the global liberalization and free circulation of people, goods and ideas (Stern, Jessica, 1999). Today, thirty years after the introduction of the term, the concept of cybernetics, it inevitably became a primary component of many important terms: cyber society, cyber policy, cyber economy, cyber warefare, cyber terrorism, cyber crime, in which essentially the most precious crown represents cyber information. Cyber terrorism is an important cybersystem of cyber warefare, and is very difficult to detect and counter because it is almost impossible to determine the political affiliation or sponsors of its prepertators.

**Keywords**: cyber; spase; terrorism; attack; warefare;

***Phd.Cand. Jasmin Kalac**

Macedonia, Gostivar
International VISION
University, Faculty of Law

**e-mail:**
**yasmin.kalac@vizyon.edu.mk**

**Article type:**
1.02 General scientific articles

**UDK:** 323,28:004]:355.45

**Date of received:**
June 19, 2017

**Date of acceptance:**
July 21, 2017

**Declaration of interest:**
The author reported no conflict of interest related to this article.

## 1. INTRODUCTION

The construction of modern and flexible computing and communicating systems set TCP/IP protocol as a universal communication protocol provided information around the world to move with incredible speed, delivering all the events in a new dimension of communication called cyberspace. The new forms of warefare and terrorism as a specific, modern “form of warefare” will co-exist at the same time with “cyberspace” attacks. The cyber warefare is directed towards the information and information systems that provide support to the civilian and military structers of the opponent. It enteres the sphere that is much more subtle than physical attacks and destruction or the acts on the flow of information in networks and manipulate them (interrupts, change its form, adds, etc.).its activities are geared primarly to information are crucial for the functioning of the civilian and military systems and air traffic control, commodity exchanges, international finansial transactions, logistical needs and goals. The opportunities for disruption of national computer systems and the ability to threaten the normal pulse of the social life and the dangers of mass endangering the lives od the people contributing the term “cyber terrorism” to be surrounded by sense of fear and wraped in the veil of mystery (Kotovcevski Mitko, 2004 god.).

More expansive conceptions of cyberterrorism as any form of online terrorist activity unsurprisingly tend to be associated with a higher estimated probability of the threat’s materialisation than do more restrictive accounts (Stuart Macdonald, Lee Jarvis, Tom Chen and Simon Lavis, 2013). One of the most sustained deconstructions of the cyberterrorist threat is provided by Maura Conway (Maura Conway, p.11). Terrorists, she notes, are routinely dehumanised, while technology is associated with a lack of control over the world. The combination of these spectres is, therefore, ripe for the establishment of worst case scenarios in which entire societies are ‘cut off’ and thus rendered vulnerable by the ‘evil’ of terrorists (Gabriel Weimann, 2005). If information warefare, without a doubt, represents a way of warefare in the future, then and the future of terrorism will be substantially determined by the emergence of cyber terrorism. The attraction of the warefare of information sponsored by the state is so great that many nations will not be able to resist this “challenge and tempation”. However, cyber terrorism in the future will represent a new “fatal attraction” for a number of terrorists and terrorist organizations. This terrorism is the most clear example of the globalization of the world, but also its “outside marriage mischievous child”, which dangerously endanger the communications in the military sphere, emergency medical care, traffic systems from different types, telecommunications and other goods. Also, its “hacker games” can cause chaos and anarchy through attacks on bankers and other financial and computer links and totally paralyze life in the big urban centers of the most developed countries. (Badey, Thomas, 2005)

In their wide range of activities include the use of private information to export same forms of cyber crime by entering into networks, as well as physical and electronic destruction of digital information system. Already there is no digital device that can not become a victim of computer vandals and terrorists.All devices connected to computers may become a target for hackers, who through a global computer network can bring a digital code that would violate their regular and normal operation. On any device that connects to a network can send an arry of digital commands that will make the device work as the creator wants those commands. The classical protection systems are virtually helpless in the methods used by today’s hackers and cyber terrorists.

The main danger today represent the hacking codes that use every occasion to implement in a closes computer network created by making themselves can be activated and the effect still be scarier, themselves finding their way to breeding, spreading the “evil code„. Also, printers become more sophisticated, upgraded with numerous software applications for support could be used for terrorist cuber hackes intrusions into networks.” (Tuchman, Barbara; 1967)

## 2. METHODS OF CARRYING OUT THE CYBER TERRORISM

In societies of the third technological revolution there are two primary methods through which terrorists can carry out terrorist attacks.The first method is when the information technology represents a target of terrorist attacks. So the carrying out of certain sabotage (electronic and physical) on the information system, will try to destroy or to commit stoppages of information system and information infrastructure, depending on the specific goal. ( White, Jonathan; 2003)

The second method is when the information attack is a tool-step for implementation of more operation. This act implies that terrorists will make efforts for manipulation and exploration of the information system, theft of information as an alternative or forcing – “programming” of the system to carry out the function for which is not intended.

Under the term computer virus refres to programs that negligent individuals write to inflict greater damage on many computers connected in a network such as the goal Internet-network. Their main features are: to copy themselves on a computer that would come in contact. They are not detectable or mostly invisible to the computer user, especially if the computer is not installed a specialized software for their detection. They automatically carry out certain commands like deleting useful data on the victim’s computer, or send data to a specific location on another network without knowledge of the computer owner. Besides hackers and groups that they organize for unauthorized instrusion into protected systems, nowadays there are specialized government secret services by entering the computer system of other countries obtain data of destructive nature. Thus under the term computer espionage can be defined as one of the modern forms of intelligence but there is also an industrial espionage that is only of a commercial nature. Computer sabotage have in case when someone destroy, delete, alter, conceal or damage the computer which is important for the state authority, institution, public service.

The attack by information technology is easily feasible, by using cheap assets that are easy yo hide and are virtually unreachable. Is it is known that terrorist “go crazy” about their media promotion, if it is known that the most desirable target for terrorist is the media, then certainly we can conclude that the possibilities of terrorists undisturbed intrusion in sensitive information technology enormously increases their opportunities for “information warfare”. That is just another perfect weapon in the rich arsenal of weapons to terrorists who tirelessly follow all modern trends in this important area.

If today there are a huge number of objective and subjective obstacles of starting a cyber war of major proportions (for example: international economic dependency, escalation and response from the other side in a military conflict, lack of technological rediness), then the new “terrorists” there are no obstacles not the “red line” for launching cyber terrorism globally.

The invisible armed enemy only with a lapto, PC, connected to the global computer network, “armed” with vast human knowledge being transformed into a digital code that decides enormous destructive power and fiery desire to achieve their dark goals, sails into attack with difficult recognizable direction, but with a single objective: electronic attack on national information network of enormous strategic significance for smooth functioning of all vital social functions (www.ict.org.il).

It is ominous face of cyber terrorist and cyber terrorism, a dangerous threat to the national security of certain countries, a death threat to global security in the future. It is close to the danger of atomic bomb. The invasion of cyberspace countinues at a rate of speed of a powerful offensive computer technology. The world again is facing a new and more dangerous serious security challenge of the greatest evil – terrorism.

## 3. GOALS OF CYBER TERRORISM ATTACKS

Nowadays, most modern weapons is the computer. Everyone well trained computer user is a good soldier. Any child who well understands the concept of the computers and the method of work of some programs is a potential danger for whole world. In the world there are many examples of computer attacks, in which victims of such attacks are various companies or government institutions. The question is what is the purpose of such attacks? In many cases with such attacks are stealing information from military institutions that directly threaten the security of a particular country. In other cases codes are being stealt from some programs that are in development, and third cases the attacks are carried out just for fun (or training). This will be investigated through examples of computer attacks that are attacked servers from one country by computer users to another country.

In 1999 IRA shocked the English public with treats that despite the bombings and other forms of terrorist attacks will start to use electronic attacks on government officials and computer systems.

Experiences with Al-Qaeda have also shown that the members of these terrorist ogranizations now use sophisticated techniques to protect their channels of communication through the Internet, setting a new daily web sites on which propagate their fundamentalist ideas, and some of the arrested terrorist are found computers with codified files. (Spisanie, dekemvri 2001: Odbrana br.68)

The attack on the World Trade Center in New York we all know how it ends. However another thing was interesting. Immediately after the attacks, the official site of the World Trade Center was blocked. It is hard to call this coincidence.

Shortly after the attack, the US feared of a repeat attack, but this time a computer. According to US experts, the success of such attack whould paralyze the country. For their luck such attack did not followed (at least not successful).However of the preventive measures, the Pentagon was “disconnected” from Internet. USA was preparing for “electronic Pearl Harbor”. The damage from such an attack would be invaluable. In fact a few years ago in the USA, certain Robert Moris, son of some of the directors of the National Security Agency, in the network inserted a programe that fully paralyzed the computer in some of the most important federal university institutions (for that he got a sentence of only 10 000 dollars and 3 years of conditional imprisonment) (http://www.terrorism.org/).

A distinctive “cyber” war was waged between China and USA in May, 2001 (the reason was the clash of Chinese airplane with American spy plane). Immediately after the clash began the attacks firstly by China. Goal of such attacks were the servers accros USA, and the site of US Congress suffered. It is characteristic that in these attacks are not being made some major damage, but only modified contents of certain pages (usually a Chinese sybols were written out).However the hackers from USA remained bound on these attacks. They responded with attacks on the websites of provincial governments in some of the provincies in China, as well as the Korean companies Smsung and Desoo Telecoma (interestingly, in this “cyber” war on the side of the Americans were Hackers from Saudi Arabia, Pakistan, India, Brazil, Argentina and Malaysia, and the side of Chinses hackers were from Japan, Korean and Indonesia). It was obvious that the states have financed such attacks, because the two “major” hackers were responsible for preparation of the servers in the US of possible attacks. (Bogoev, 2010)

On July 1, 2001, in Mexico was arrested a Mexican teenager who was accused of committing an attack on NASA. He managed to get into the server, modified some files and created some illegal accounts. It is interesting that in defense the Mexican teenager defended himself by saying that had nothing to do with computers, and that he is by mistake accused. Does this country wants to instill fear among hackers for their successful presecution, whether the state is served by false accusations? Why are these false accusations?

## 4. CONCLUSION

Legally, cyber terrorism is an international abuse of the digital information system or network components that completes or combat the terrorist activity. The consequence of the abuse of the system will be direct violence against people (which is not excluded for example airplane, chaos in hospitals, etc.), but can cause fear, increasing world crime with fastest pace, the greatest strategic vulnerability of all vital social functions, enormous human suffering and victims as “collateral damage”. In this context, even worse is the fact that these subtle effects may initiate cybernetic was or “place” certain states to start classical war, in response to cyber actions “taken by the other side”. Under certain US considerations it is only a matter of time before the US can experience “cyber pearl harbor”, which would have devastating results, thefts of electronic funds of data that would supported the terrorist information, remitting, diverting consignments of weapons, etc. But, probably the most dangerous is the eventual simulation of “Cyber Chernobyl” disaster.

## 5. BIBLIOGRAPHY/ REFERENCES

1. Badey, Thomas (ed.). Violence and Terrorism 05/06. Dubuque, IA:McGraw-Hill/Dushkin, 2005.p.152
2. Богоев Славчо ,**Колективните системи на безбедност: процес и критериуми на интеграција на Република Македонија во НАТО**, Правен факултет, 2010 стр 63
3. Maura Conway, “The Media and Cyberterrorism”, p. 11.
4. Gabriel Weimann, “Cyberterrorism: The Sum of All Fears?” *Studies in Conflict and Terrorism* 28 (2005), pp. 129-49.
5. Митко Котовчевски “Борба против тероризмот”, Македонска цивилизација -Скопје.str 182
6. Tuchman, Barbara. The Proud Tower. New York: Macmillan, 1967.p.52
7. White, Jonathan. Terrorism: An Introduction. New York: Thompson-Wadsworth, 2003.p.89
8. Stuart Macdonald, Lee Jarvis, Tom Chen and Simon Lavis, (2013) *Cyberterrorism: A Survey of Researchers*. Cyberterrorism Project Research Report (No. 1), Swansea University. Available via http://www.cyberterrorism-project.org (accessed 28 June 2013).
9. Stern, Jessica. The Ultimate Terrorists. Cambridge, MA: Harvard University Press, 1999.p.204
10. http://www.terrorism.org/
11. www.ict.org.il