DE GRUYTER OPEN

International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXII No 3 2016

THREAT ANALYSIS IN THE NETWORK-CENTRIC ENVIRONMENT

Mirosław SMOLAREK*, Marek WITKOWSKI**

***Baltic Defence College, Tartu, Estonia**
****The General Tadeusz Kościuszko Military Academy of Land Forces, Wrocław, Poland**
miroslaw.smolarek@baltdefcol.org, m.witkowski@wso.wroc.pl

***Abstract**: The paper presents an analysis of the threats that one can face in the cyberspace and dangers affect the safety of a state and its citizens. The authors compare definitions of terrorism, particularly focusing on issues related to cyber terrorism. They explain concepts associated to terrorist activities in the network-centric environment. Next, the evolution of the threats awaiting in the Internet has been presented. Moreover, classification of cyber-attacks and current dangers that may occur in ICT systems has been analysed.*

Keywords: Cyber terrorism, cyber threats, network terrorism, Information and Communication Technology (ICT) systems

1. Introduction

Cyber terrorism is quickly becoming a serious problem, which now have to face almost all the states of our globe. Cyber threats are evolving with the development of the Internet and the increasing importance of transmission of electronic data, "addiction" of the modern world to rapid information transfer. Network-centric environment influences more and more areas of human life, including military aspects. Analysis of cyber terror activities clearly shows the existing problem that absolutely must be fought. Vulnerable to attacks are not only networks of important international and state structures, private companies, but also the computers of individual users. Regardless of the place of attack, all users must realize that their important data, private photos, programs, research work, which are gathered in the multimedia devices connected to the Internet networks - are vulnerable to theft and use for different purposes (commercial, blackmail, espionage etc.). In addition, free access to the network and IT systems means that terrorists use them to promote their ideology and recruit new supporters world wide. Via the Internet terrorists not only gather information about targets of their future attacks, but also by wide Internet networks they can communicate with their supporters and followers around the world and issue orders to the members of such illegal or clandestine organisations. Therefore, all IT users should be aware of current threats, which can be implemented via the Internet. One should be aware of current threats, which can be implemented via the Internet.

2. Cybernetic face of terror

The first serious "battleground" in cyberspace was Estonia, which was attacked by the Russian organization "Ours". The denial of service (DoS) type attacks on government services took place

DOI: 10.1515/kbo-2016-0095

after 22.30 April 27, 2007. The apogee of the cyber-attacks took place on May 9 in the Russian Victory Day, when overpowered been not only the most important state institutions, but also the private sector. Only after three weeks (18 May), attacks on Estonian IT infrastructure have been finished. [1] Incapacitation of organizations and institutions via the Internet showed how serious threat to national security are the terrorist attacks in the net-centric environment. The Estonia example showed a need for redefining definitions and methods of coping with the new terrorist threat.

The perception of terrorism have changed always and took on a new meaning after the serious terrorist attacks e.g. in 2001after 9/11 events in USA. After such occurrences definitions of terror and terrorism evolve also. There are ca. 120 definitions. Let present only a few of them, which should be enough to understand the concept of such evolution.

The word "terror" comes from the Latin "terrore" - terrify and means the use of violence, rape, cruelty, repression, threats. After the 9/11 attacks, the European Commission proposed a uniform definition, according to it terrorist acts are "…offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of seriously intimidating a population, or unduly compelling a government or international organisation to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation…".[2] According to NATO terrorism is "The unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives ".[3] Quite interesting definition proposed B. M. Jenkins to define terrorism as "…the use of criminal violence to force a government to change its course of action, usually to withdraw from or desist from undertaking something. It puts pressure on a government both directly and through overt threats and actions, and indirectly through instilling fear in the population". [4]

Above mentioned definitions fit to actions conducted by the cyber-terrorists, that is why one can count cyber-attacks as the phenomenon related to terrorism. Modern threats lurking in cyberspace has become the most dangerous contemporary phenomenon posing a threat to the democratic states. Of course still spectacular "conventional" terrorist attacks which the entire globe could observed in Paris and Brussels last March, with the large number of victims, gain more publicity and media attention, however the case of Estonia has shown, that the cyber-attacks could have much more severe consequences for the state security and national critical infrastructure. Of course e.g. terrorists could try to bow-up heavily protected nuclear power plants in order to cause radiological contamination on the Chernobyl scale, but the example of hampering Iranian nuclear program by destroying the centrifuges for Uranium enrichment by the virus Stuxnet [5] in 2010, showed that it is probably possible in the nearest future to achieve similar effects by cyber-attacks in easier and much more effective ways. Moreover in case of the cyber assaults there is no need to be or use the territory of the afflicted countries or in the physical vicinity of the attacked facility or installation. This fact makes very difficult the protection of the critical infrastructure against such attempts.

Let's try and define the phenomenon of "cyber terrorism" the word was first used in Sweden in 1979 in the report about the dangers of use of computers [6]. Under this concept, they understood any activity related to use of computers interconnected by telecommunications networks intended to destroy: computer systems, control and supervision systems, programs, data, and

consequently bullying governments and societies, exert psychological pressure. Even the report mentioned the threat to life or possibilities of causing huge material losses, resulting from terrorist activities in the cyberspace. Then in the '80s the word cyber terrorism was used by American intelligence society, pointing out the possibility of carrying out electronic attacks by the enemies of the United States. Already in 1998 the Center for the Protection of National Infrastructure (NIPC) at FBI headquarters was created, which main task has been coordination of the activities relating to collecting information in order to respond to threats or attacks on critical infrastructure of the state. After the 9/11 politicians and public media drew attention to the possibility of further terrorist attacks around the world, but also warned of the possibility of occurrence of massive cyber-attacks against information systems of the United States and countries allied in the fight against global terrorism. The increasing number of cyber attempts aroused the interest of scientific society. Until now the concept of cyber terrorism has not been defined completely. NATO even does not have any definition of "cyberterrorism". One can find only a definition of "Computer network attack" in which only cyber-attack is mentioned but there is no further development of this issue. Computer network attack is "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber-attack."[7]. One can find many definitions of this phenomenon, but they differs from each other, depending on the creator. The scholars carry on stormy discussions about the issue, particularly among those dealing with security systems. Generally, cyber terrorism – could be defined as actions aimed at: interception, modification or destruction of information transmitted in ICT systems. The authors of this publication assume that cyber terrorism is a combination of traditional terrorism with cyberspace. Therefore, analysing the concept of cyber terrorism, it has to be an attempt related the unlawful attack or the threat of such attack, conducted through the IT network usually via the Internet. The aim of such attacks is to provoke fear among average users, specific groups, organizations or institutions that use a network or the Internet connections. Such measures are taken in order to intimidate somebody or force satisfying somebody's political, social or financial demands. In addition, some authors present an innovative approach to the definition of cyber terrorism stated that for qualifying such an attack as a "cyber terror", it should "result in violence against persons or property, or at least cause enough damage to cause fear". Examples could be attacks causing death or injuries, explosions, aircraft disasters, water pollution and severe economic losses. However, serious attacks on critical infrastructure can be count as "cyber terror" according to their effects. However "…cannot include attacks that disrupt nonessential services or cause primarily financial trouble." [8] Regardless of the definition, it must be assumed that cyber terrorism is not a separate or specific type of terrorism because of ideology. It serves exactly the same purpose as bombings, kidnapping of airplanes or taking hostages. It is only different in the means and ways of the criminal activities in which the modern technology has been used due to increased access to the Internet.

The introduction of the new weapon which is cyber-terror changed dramatically the situation of the terrorists and their organizations. They set up a new powerful weapon which in addition to traditional terrorism (e.g. the destruction of manpower, goods produced by humans, installations) allow them to spread havoc on a global scale. The cyber terrorists know that the infrastructure of each country very often based on the Internet connections, is heavily dependent on multimedia devices and sometimes additionally connected to a

local (LAN) or wide area networks (WANs). This situation caused that the terrorists can direct their criminal activity at users who use modern technology and IT infrastructure.

The new threat re-defined the tasks of all national and international organizations and agencies responsible for security. Their "traditional" main tasks regarding combating terrorism include:

- recognizing of the terrorist groups and their members, detecting their links with international organizations;
- operational activities in areas relating to organized crime activities (smuggling, human trafficking, arms, ammunition and explosives trade);
- limiting the possibilities of financing of terrorism by indigenous criminal organizations, as well as the elimination of capital flows and money laundering;

Another important area of combating terrorism is prevention. The most important preventive measures are among others:

- organizing physical security of the most important state facilities, critical infrastructure installations, governmental and administrative buildings, financial institutions, and all other strategic objects;
- ensuring safety of the public transportation, e.g. airports, railway and metro stations, etc.;
- prevention against NBC- or bioterrorism;
- border protection and infiltration of incoming refugees or even visitors from regions known as supportive for terrorism;
- explaining the reasons of actions and informing the society about potential threats, allowing the correct public perception of increased preventive measures.

As was mentioned above, in '80s of 20th century the agencies got new important task which was protecting states and society against cyber-terror activities.

3. Cyber threats

Development of cyber-terrorism has become possible with the unlimited public access to modern equipment and multimedia services which has enhanced use of the Internet. The services become more attainable, the terrorists get easier access to them. Moreover, the increasing number of users and the availability of various services, often paid, causes the threat that disruption of this type of communication and delivery of services can cause serious financial losses. Cyber-attacks are quite safe for their performers, because they may carry out such attempts from distant corners of the globe, which significantly limit the possibility of detection of terrorists. In many cases the cyber-attacks could be classified as "normal" criminal activities, but their scale and effects are much larger. The main objectives of cyber-attacks are: financial operations (including the stock exchange and e-banking), telecommunication networks, control systems, electricity supply, traffic control centres (e.g. transport by land, air and sea), military agencies and installations as well as state organizations, institutions, and public safety services. Cyber terrorism is even more dangerous for modern and well-developed societies, which are much more dependent on information technology. Therefore, there is no doubt that the information, which has become an economic category, is and will be, increasingly the cause of many conflicts and the technology will be used for particular purposes. In addition, services and ICT equipment can be excellent tools for warfare, which can be carried out in a network-centric environment, but the results and consequences of such "skirmishes" will influence the real world. Cyberspace allows to conduct conflicts but at far less cost and with grater final effects. Moreover, in the case of such cyber war, it becomes irrelevant the level of training and professionalism of "old-fashioned" type soldiers, weaponry and technology but the results will depend on skills and level of knowledge of "cyber-warriors". Hence recruiting the best hackers will be the beginning of forming new type "cyber-

armies". The ability of their soldiers possessed information resources will determine victory or defeat. This process has been already initiated in some countries.

4. Evolution of threats and methods

The development of IT systems, introduction of IT networks and the progressive computerization, facilitated fast access to knowledge resources and contributed to the rapid development of the humankind. Computers dominated almost every field of human activities. They control the production processes, support the energy supply, manage financial services, aviation, communications only to mention some of the areas.

The emergence of computer technology and its use in everyday life occurred only several decades ago, and since this is also the time one can speak about the appearing of related dangers. At the beginning there were no serious threats, because the use of computers was not as wide as currently. In the '70s, after introduction of open network systems, and the proliferation of personal computers, the problem of IT crimes has become a real danger. Personal data has been copied and processed extensively, not only with good intentions. Hackers were motivated by various factors: the desire to test their capabilities, challenge, enjoyment, financial benefits. There have been a number of computer frauds, acts of economic espionage, as well as crimes of criminal background (illegal copies of programs, counterfeiting of magnetic cards, hacking etc.).

It was only in the '90s in a period of rapid development of computer networks and increased interest in the Internet, the phenomenon of cyber terrorism began to be treated with due attention. For hackers a thrill of emotion was not enough, their aim were piracy, theft of trade secrets, forgery, destruction of data, and even sabotage of information resources.

At present, the phenomenon of computer crime and the use of ICT networks for criminal purposes are gaining momentum. Breaking into computer networks, their penetration and theft of data, involve a huge consequences, not always giving miscalculate in the economic dimension. The aim of such attacks can be important national and international security institutions (police, military, government, telecommunications), which may result in paralysis of the critical infrastructure of the state or be the cause of a significant weakening its effectiveness. For the hackers a new cyber world opened up with new opportunities and insufficient protection of IT systems contributed to their penetration.

Many talented programmers drifted into crime (Mitnick, Poulsen, Zboralski, Morris, Lamo). Even though about the existence of some hackers one can hear in the media, read on websites, but the best of them are working in secret, for big money, for great powers, intelligence institutions and… terrorist organizations. They are searching for important information, acquiring data by some are impossible to get. They leave no trace, constantly monitor the systems in search of strategically important data and targets, waiting for the right moment to strike and destroy the entire infrastructure of a state or region with the help of computer keyboard from anywhere in the world. Also terrorist organisations have increasingly began to use modern technology to achieve their objectives. They use networks and ICT systems to coordinate actions, to carry out financial transactions, to exchange encrypted messages, such as maps, operating instructions, targets of attacks. For these purposes, they use the most sophisticated achievements in the field of computer science. As an example one can mention steganography. This is the technique of hiding additional information within any file. It can be a picture, text, digital video, MP3 music, or even application. Original illustration of seemingly does not change - it can be viewed and edited. The attached hidden information does not increase even the

volume of the file. In this way, one can transmit classified information looking as quite "innocent" e-mail attachments. The message could be also encrypted with a private key. To capture such hidden message, one should already know where to look for it. The existing procedures and mechanisms for capturing encrypted information are helpless in the case of steganography. Moreover the Internet is also used to spread a terrorist propaganda and ideas, recruit new followers, to communicate between members of terrorist groups, sending threats, and to carry out attacks on networks and information systems.

5. Classification of cyber-attacks and threats

After the attacks on the WTC and the Pentagon a special report was prepared in the United States, which has also forecasted possible cyber terrorism threats. The report pointed out the three forms of cyber-attacks: propaganda and disinformation (unlawful modification web pages, ideological spamming), computer sabotage (denial of service attacks, distribution of viruses, worms and other malicious computer programs) and attacks on critical infrastructure connected of interference in its functioning. Typology of cyber-attacks presented in the report could be a good starting point for a reflection on the essence of the concept which is the subject of this analysis.

Technological progress and the rapid development of the Internet has become not only a source of knowledge and its broad capabilities for data exchange, but also allowed increasing of losses for its users. Constantly new forms of cyberspace attacks are creating which can reduce productivity, cause downtime or lead to losses of important data.

The primary threats for IT systems are viruses, Trojan horses, and worms. Even the less destructive of them can decrease productivity and those whose aim is the destruction can modify data, delete them or damage applications. Very often they use security holes in operating systems and applications. As a result, they can spread without human intervention and knowledge. Another threat is represented by people wishing to gain unauthorized access to systems, commonly called hackers. Amateurs predominate among them, who are not able to cause a loss or even gain such access. However, there is a small group of people with extensive knowledge and practice not only IT, but also e.g. in psychology, who try to gain access to IT systems because of different reasons either to test themselves or for material gains. The last category of threats to data security and computer systems are people employed in a given institution. They have the easiest access to computer systems and are able to damage them physically, delete data or modify them for their own benefit. Modifications of data are easiest to carry out for IT department employees who have the quite unrestricted access to applications, databases or even personal desktops of users. Laying off employees, specifically fired by the employer, is also a high risk. Grievances sometimes directing their actions, they can intentionally upload viruses to internal networks and also destroy or steal sensitive data.

Attacks in cyberspace can take different forms - from emailing a virus, hacking into IT systems, destabilizing them to take complete control over them. Thus, the IT system may be attacked in a variety of ways. This may include: passive and active attacks.

Passive attacks – based on eavesdropping or monitoring of transmitted data. Such attacks are very difficult to detect because they do not make any changes in the data. These in turn can be divided according to their type:

• social engineering - a set of ways to phishing passwords, accounts and other elements affecting the security of computer systems;

• capturing of passwords - each user has his own personal account to which only he has access;

• scanning - penetration test on a computer, in order to gain information about the architecture, the type and version, operating system and the services offered;

• sniffing - technique of eavesdropping packets flowing on the network. Frequently it is capturing the entire session, network traffic and its analysis in terms of selected information;

Active attacks - as opposed to the passive ones, rely on the modification or creation of false data. These in turn can also be divided into several types:

• replay - the interception of data and its retransmission, in order to obtain illicit results;

• spoofing - rely on impersonating another user authorized to make the connection (IP-spoofing and DNS-spoofing);

• hijacking - causing interruption of the connection set up between the client and the server, and then impersonate the client and the server to send its own sequence numbers;

• buffer overflow - use programs called exploits for modification of the memory buffer in order to access the resources. The aim of such an attack is to run a remote shell, which will be used for the real attack. This action allows the attacker gaining the ability to run their own code on a victim's rights process, which until now has been run by an authorized user. To achieve the best possible results of his/her actions, the hacker usually selects the processes running with administrator rights. Such an attack is possible when the server software application contains logic errors used by the hacker;

Denial of Service attacks - interfering with or preventing normal operation. Due to the types, there are three effects of his actions:

• destruction of resources - the collapse of the system or bring it to unstable state;

• denial of services - reject connections for a certain time;

• exhaustion of resources - such as overload of memory, processor capacities, etc. which may block the computer;

☐ Trojan horse – is a programme which helps to overcome a system security by bypassing the authorization procedures. Trojan horse may be holed up in virtually any program and it is very difficult to detect, because it operates in the background without revealing its activities. The most popular is the Trojan horse Backdoor / Sub-Seven, which takes control of the infected system and causes extensive damage in it. In addition, Sub-Seven can launch and close programs, break online sessions, as well as manipulate the content used data, download screenshots and change its content (display pop-up windows, manipulate the data directly on the screens of the application), eavesdrop online sessions and even remotely modify the Windows registry.

Other examples of Trojans are: ~Bladerunner, NetBus, Back Orifice, Deep Throat, Trans Scout and many more;

☐ worm - self-replicating program that spreads through the Internet, causing additional overload of the network and damage in infected systems. They represent a very serious threat and one can observe increasing damages caused by this type of the program. The most known worms are Iloveyou, Novarg and Mydoom;

☐ virus - is probably the most popular and most widespread threat for IT systems. One of the virus definition says that "it is a piece of executable code, incapable of independent existence and endowed with the ability to reproduce." Viruses can cause

a variety of unusual and undesirable actions in our system, beginning with the display harmless messages or written threats on the screen, and ending with the complete destruction of data and immobilization computer.

Viruses can be divided into the following types:

• boot-sector virus - attacks the significant initial area of storage or hard disk. The virus can attack from an infected

disk structure every time if someone starts the computer;

• file virus - infects executable files (.exe, .com, etc.). Usually every time when somebody runs an infected program, the virus replicates;

• macro viruses - a very common type of virus. Microsoft Word and Excel perform a series of instructions automatically when opening documents. If a text or spread sheet will be equipped with a malicious macro, one can expect a loss or destruction of contents of the open file;

• complex virus - uses a combination of different techniques to spread in the system. The most common is a hybrid file virus and a boot-sector;

• poly-morphic virus - the code is changed automatically with each infection. To detect it is necessary to use heuristic methods;

• stealth virus - uses a variety of techniques that hinder the disclosure of its presence in the system;

• "zoological" virus - stored in the collections of viruses in researchers laboratories. Often ineffective, unparalleled "in the wild";

☐ logical bomb - causes damage to the system processed data;

☐ attack on a password - one of the most primitive methods of hacking into various systems. The ability to cracking a password is a preliminary step for any hacker. This is partly due to minimum of IT knowledge and expertise. For more advanced intruders breaking passwords frequently is the next step after obtaining the basic access to the system. It allows them to exponentially increase the user rights, and thus improve the effectiveness of the attack. This occurs very often and it is associated with the use of so-called weak passwords. Common type of breaking is use of so-called dictionary mode, which is based on the defined database of words, creating possible strings and sequences.

The above presented types of the cyber-attacks show how many threats are lurking in the virtual space and new ones are emerging in sophisticated forms and varieties. Attacks carried out by viruses and network worms seem to be a great weapon with which the economy of many countries may be severely damaged.

There are a lot of possibilities of attacks on ICT systems. Currently no system is 100% safe. Technological progress is growing at a dizzying pace, so that security and technology must keep pace with these changes.

6. Conclusion

There are many threats that may affect ICT systems, causing interference or even incapacitation of networks of international and national organizations, private enterprises and ordinary users of multimedia devices.

The network terrorism will not replace the traditional forms of the terrorism based on physical violence, but it will be increasingly effective in supporting terrorist activities. Terrorists will use attacks on ICT systems (government networks, communications, energy) to spread terror and enhance the effects of their attacks. Terrorist organizations use the most sophisticated achievements in the field of IT systems for their illegal activities and they increasingly will use this knowledge to achieve their political goals. The number of attacks in cyberspace increases from year to year, so the problem of IT security should be taken seriously and there is a need to develop effective methods to combat cyber terror. Lack of protection systems against cyber terrorism in some countries or underdeveloped IT security systems can cause that terrorists will use IT infrastructure for its own purposes, causing disruption and chaos in society. Therefore, all users of IT systems should be informed about current dangers in cyberspace and indicate ways that will minimize the effects of potential cyber-attacks.

References

[1] *Russia accused of unleashing cyberwar to disable Estonia*, http://www.theguardian.com/world/2007/may/17/topstories3.russia

[2] *Council framework decision on combating terrorism*, Official Journal of the European Communities (2002/475/JHA).

[3] *AAP-06 NATO glossary of terms and definitions*, NATO Standardization Office, 2014, 2-T-5.

[4] B. M. Jenkins, *International Terrorism. The other world war*, Santa Monica, RAND, 1985.

[5] K. Zetter, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[6] M. J. Littleton, *Information age terrorism: toward cyber terror*, Naval Postgraduate School Monterey, 1995. http://fas.org/irp/threat/cyber/docs/npgs/terror.htm

[7] *AAP-06 NATO Glossary of Terms and Definitions,* NATO Standardization Office, 2015, 2-C-11.

[8] A. Podraza, P. Potakowski, K. Wiak, Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Warszawa, Difin, 2013.