CYBER TERRORISM AND CYBER CRIME – THREATS FOR CYBER SECURITY

Jugoslav Achkoski
Military Academy "General Mihailo Apostolski " - Skopje, jugoslav_ackoski@yahoo.com
Metodija Dojchinovski
Military Academy "General Mihailo Apostolski " - Skopje, m_dojcinovski@yahoo.com

Abstract

This paper has aim to give contribution in supporting efforts against cyber threats recognized as a cyber terrorism and cyber crime. Also, it has aim to show future challenges related to cyber security and their emerging threats – cyber war, cyber terrorism and cyber crime.

Accelerate weapon development called ICT (Information Communication Technology) which is developed every day faster and faster, and development of human conscious on higher level about consequences of ICT enormous penetration, contributes to emerge new threats in cyber space.
Comparison between conventional weapon and cyber weapon proves that hardware presents assets, which is used for bullet to be thrown out, and software presents bullet on itself that can causes damage or puts down harmful consequences.

New threats known as a cyber war, cyber terrorism and cyber crime cause significant disruption of cyber security in cyber space. We can firmly conclude that if ICT becomes more sophisticated subsequently methods and assets use in war against this type of asymmetric threats become more complex, focusing on cyber terrorism and cyber crime.

Keywords: *cyber terrorism, cyber crime, cyber security, cyberspace, Information System*

Introduction

World in this time of enormous technological development has many challenges in fight against phenomenon of cyber threats, especially cyber crime and cyber terrorism as a new forms of asymmetric threats in 21st century.

In order to protect security system by emerging threats – cyber terrorism and cyber crime, mainly on national than regional level, is needed to be taken appropriate activities. Protection from cyber crime and cyber terrorism is related to protection on all spheres which have near points with that activities.
Reason for emerging this kind of threats is technological development, which brings certain changes in society and as a consequences are ICT penetration in all spheres in society.

Because of all previous mentioned reasons, cyber security should assist to be established mechanisms in fight against this kind of asymmetric threats not only in the region but also worldwide.

1.Cyber space

One of the many national strategic objectives which should be written in Strategy of defense for countries in general term, it is cyber space protection in order to protect critical infrastructure and decreasing possibility of intrusion and cyber attacks but also reducing damage consequence caused by cyber attacks.

Furthermore it is necessary to emphasize that government services depend on cyber space in the meaning that they "fly" in that space, because they offer services in banking, finance, healthcare, information and telecommunication services and other fields.

The US Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology

infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (JP 1-02) (Wills, David, and Bunn, Sarah, 2006).

According to previously mentioned reasons, security in cyber space is most important because of permanent use of governmental services and increase of public trust in information systems. In order to accomplish aim, it is necessary to establish new level of communication and cooperation not only between governmental agencies and departments but also government and private sector (G2B).

Mentioned above affords to conclude that is necessary to protect national critical infrastructure from intrusion and cyber attacks for the reason that hackers and other intruders can firmly use critical infrastructure as tool to perform their attacks. Optimal communication in cyber space is significant in order to exchange information between linked governmental institution. High-quality connections between institutions affords accelerate detection in addition to solve IT problems, known as viruses or other types of cyber attacks.

IT infrastructure through strong control security mechanism is a "first step" to sharing information in timely, efficient and reliable manner. Security policy and strong secure mechanisms meet the requirements of sharing sensitive data which affords to government authorities to give quick answer, next make right decision and coordinated activities in critical situation.

2.Cyber crime

Cyber crime encompasses any criminal act dealing with computers and networks. Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet (Forno, F.R., 1998).

Some attacks in cyber space do not have certain targets, because attacks against computers or group of computers are becoming more common. Home users of computers, organizations either private or governmental can and their information technology networks can be target of attackers. Moreover, attackers using computers can cause damage to Critical National Infrastructure (CNI) that includes emergency services, energy distribution, health, finance and anything which depends of IT. Many IT systems which were isolated from the internet, now they are connected to internet and level of their violability become bigger.

There are two main ways by which computers can be involved in crime (Schudel, Gregg, and Wood, Bradley, 2000)

- old crimes conducted using computers as a tool: for example storage of illegal images on a hard disk instead of in print; harassment using mobile telephones or illegal downloads of music and other forms of piracy. Another example is 'phishing': confidence tricks involving spoof emails and fraudulent websites to acquire sensitive information. (Freeh, J.L., 1998)
- new types of crime made possible by specific technologies. One example is denial of service attacks or DoS which prevent computer resources being available to intended users, for example by flooding web servers with more data than they can process, thus forcing websites offline. Other crimes involving attacking a computer (often by 'hacking' or gaining unauthorized access to a computer system), or writing a virus (a type of malicious software or 'malware') to delete stored data. (Freeh, J.L. 1998)

In (Computer Crime Definition, 2011), the probability of terrorists carrying out an electronic attack against the CNI is currently low compared with other risks such as using explosive devices, although the National Infrastructure Security Coordination Centre (NISCC) points out that threats can change quickly.

3.Cyber terrorism

Nowadays it is not unique definition related to term terrorism. Definitions in order to defining term terrorism has different origin, so that some of that definitions focuses on terrorism actors, but others on terrorism tactics and objectives and used methods. In order to fight against this kinds of terroristic acts or other forms of combat violence and crimes, national and international organization ask for defining term terrorism. Currently, one of the most often used definition about terrorism follows US legacy documents and policy.

According to US law, state secretary has obligation to get the report on Congress each year, which is put into Annual report. Terrorism is defined in a follow way:

"premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents" .

"the term "terrorist group" means any group practicing, or which has significant subgroups which practice, international terrorism"

According to Federal Bureau of Investigation (FBI), new phenomenon recognized as a cyber terrorism is defined by follow:

"previously planned, politically motivated attack against information, computer systems, computer programs and data that result with violence against targets that are not military (civilian) by the sub - national groups or secret agents" .

Another definition according to US Commission for Protecting Critical Infrastructure is that terrorist attacks are created in order to cause physical violence or extreme financial damage.

The cyber-terrorist is assumed to be professional, creative, and very clever. They will seek unorthodox and original methods to accomplish their goals. Individuals who are wellschooled in traditional information security techniques are not well suited to being a cyber-terrorist, simply because they have been exposed to or trained in classic security techniques and doctrine. The cyber terrorist will seek to accomplish their mission by techniques not mitigated by classic security mechanisms (Petrović R. S., 1999).

Terrorists leave traditional way of fighting with classical weapon and other weapon but also they introduce the use of sophisticated high technology which shows that they becomes "modern" warriors who take a pace with technology development. When computer terrorism is in question, nowadays there are real danger about information resources especially in global information networks, which means that if they are exploited by the terrorists, global information network can become effective weapon for cyber attacks. Also, it give to terrorists opportunities for combating in a way which previosly they can only dream abut it.

That information infrastructure is target of terrorist groups and organization shows the fact of threats addressed from Irish Republican Army (IRA) in 1997, when the English public was shocked by the threats that besides bombs, assassinations and other forms of terrorist acts will begin using electronic attacks on commercial and government computer systems

Although terrorists are recognized as a persons with psychological profile who do not have enough high level talent and high developed computer skills, but also experience with Al-Quade shows that members of terrorist organizations use sophisticated techniques for protecting their internet channels of communication, in a way which they continually change web locations in order to propagate their fundamentalist idea. Furthermore some terrorists who are arrested had encryption files on their computers, mobile phones and other devices for communication.

Danger of terrorist acts become bigger in a future because of high technology exploitation by terrorists to accomplish their destructive aims. They can performer that with "source of talents" who know how to provide experts or specialists capable to commit computer sabotage or espionage on a high strategic level.

As a result of previously mentioned, terrorist groups or organization undertaken tasks which made contracts or train terrorists to exploit high technology for secret operations or for strategic terrorism which has to be carried out by the disciplined and organized staff.

As a source of talents are recognized following groups:

- technological mercenaries;

- unemployed technological experts from third world countries;
- technological experts from developed west European countries;
- high level skill personnel from intelligence service as a Securitate (Romania), SPECNAZ and OSNAZ (USSR), Stasi (East Europe) and other units for special operations from ex communist countries in Eastern Europe

General conclusion related to cyber terrorism is that the time which follow, terrorists will use more and more high technology for espionage and sabotage also they will use it to propagate their idea.Likely terrorist targets can be the following:

- data banks;
- computer systems;
- government communication systems;
- automated power directed by computer systems;
- oil refineries;
- Airport infrastructure etc.

4. Relation between hackers and terrorists

Hacker groups are numerous and they are divide each other by the level of education in technological field. Membership in a high level educated hacker groups frequently can be limited and exclusive membership is allowed only for individuals who develop and share set of sophisticated information communication tools for hacking. This "exclusive" hacker groups make efforts to be cover and not to attract attention due to confidentiality allows them to be more effective.

Although some hacker groups can be a globally dispersed, they have similar aims as a political interest or they are connected through another basis as a religious or social ideology. Other groups can be motivated from profit which comes together with organize crime. Also it is possible to meet hacker groups which are guided from their aspiration to sell their computer skills to sponsors as a terroristic groups or countries which it is depend on emerging political interest.

As a conclusion should be stated that there are numerous reports on the above, where the actors appear as governments, companies, associations and other stakeholders. On the same manner, it should be stressed that connection between hackers, terrorist and nations that support terrorism is very hard to prove it. On other hand activities that are caused by the cyber terrorist can be detected through carefully monitoring social networks, chat, mirc and other cyber virtual location where anonymously hackers meet to exchange their information.

Nevertheless, in order to prevent and avoid damages from terrorist and crime activities are developed numerous research projects which should give contribution to find out technology, tactics, techniques and other stuff associated to cyber threats.

5. Differences between terms cyber crime and cyber terrorism

In a present time are many definitions about cyber crime and cyber terrorism. Recently was confusion whether or not this two terms - cyber crime and cyber terrorism are synonym each other. However, some authors support definition that they two terms are synonym other authors do not support that definition and they formulate two different definitions. In a global view, the most relevant definitions are definitions which are exploited according to formulate terminology of USA.

On the other hand, to make clear distinction between terms cyber crime and cyber terrorism in a following paragraphs it is necessary to be exposed differences. Defining term cyber terrorism is crucial and the officials motivate it. Major purpose of cyber terrorism is infiltration in the system on certain institution where it can cause violence and damage (financial damage, property) in order to make destabilization and lower security in the country that is victim.

Hackers that are actors which usually cause cyber crime, and they often do it for enjoyment or they struggle between each other for bigger individual success, in addition they can do it for achieving

financial or in other purposes. While hackers (cyber terrorists) who are often component of terrorist organization as a Al Qaeda, ETA, IRA etc, they make it to fulfill certain political goals (Ottis, Rain, and Lorents, Peeter, 2010).
Furthermore, some authors formulate differences about hackers that hackers who commit attacks for enjoyable reasons they can be classified in a group of simple and plain criminals while cyber terrorist should be classified in a specific rigid form of crime (Guice, J., and Duffy, R., 2000).

Cyber terrorist can attack on clear defined targets that are significant strategic points for certain countries but it does not means that attack is limited and cannot have a wide range in order to achieve definite aim. As a example of previous mentioned, target of cyber terrorist can be electrical plant which supply citizens with electricity who live in near that environment. Committing this type of attack, cyber terrorist can be effective in a wide range with a little resource. If chain of electricity supply is broken with this kind of attack that situation has influence on daily citizens routine to fulfilling essential needs (Petrović R. S., 2001).
Another example about cyber terrorism can be hospital computer system hacking and changing medical prescriptions and cause damage with prescribing wrong medicine to the patient. So that everyone can be a victim of this terrorist act (Petrović R. S., 2001).

As a conclusion about differences between cyber crime and cyber terrorism is that they use same weapon to commit terrorist or crime act and this weapon is computer or ICT in a wider range.

Conclusion

It is general accepted meaning that users of cyber space and their networks are not protected form cyber attacks. Moreover, it is not enough knowledge about cyber threats and risks and what kind of implication are caused to the national, regional and global security. However, mentioned above affords to conclude that are needed to do big efforts in developing mechanisms against cyber threats as new type of asymmetric threats.

Although some countries have technological advance and more experience in war against cyber threats and critical infrastructure protection in comparisons with others, however cyber crime is the most danger threat in comparison with cyber terrorism and cyber war. Addition threat is caused with lack of developed security mechanisms in terms of consequences which can influence to the individual users and possibility that gaps in cyber space to be exploited by the crime groups and terrorist. It is equally important which of this gaps will be used by the actors who have desire to cause violence or damage.
Challenges which appear in developing security mechanisms related to cyber security can be analyzed from different views. First, only a few nation have developed strategy for cyber security, which should give direction in order to protect critical infrastructure. Second, decreasing financial budget per current year has influence to cyber protection. Third, for individual user are not needed security clearance in comparison with security clearance and standards that are needed for institution governmental networks and networks for private sector or corporation networks.

As a conclusion it is affordable to notice that general “mixed nature” of cyber space press on defining combined definitions and standards if cyber security is developed on national, regional and global level.

Convergence of these challenges is in correlation with technological development and desire of groups, individuals and other actors to create significant asymmetric exceptions to governments or citizens in handling with cyber threats.

Generally is accepted that international organizations should lead in developing standards which will be used in selection of activities in cyber space, but there is not clear selected international organization that should be a leader. United Nations (UN) missed chance to be leader due to they cannot build consensus and all efforts in developing standards are useless related to cyber security . So that, in near future is needed to set bigger caution by the cyber community in order to discover convenient solution to handle and fight against cyber threats.

To conclude, it is accepted that cyber security is international (global) responsibility. Each user has responsibility in cyber security depending of his/her affiliation. Due to internal connections and dependences are enormous, each user in network should contribute in strengthening security mechanisms and protection form cyber attacks. As well is needed to find solution and ideas for strengthening cyber protection and increase security in cyber space as part of global strategy in order to eliminate exceptions and neutralizing threats in a wide range as much it is possible.

References

1. Advocat, Jenny, (2005) "Internet clinical trials: examining new disciplinary experiments in health care", Monash University, Australia, Anthropology Matters Journal, Vol 7 (1),
2. An introduction to e-business optimisation, http://www.weboptimiser.com/resources/index.html;
3. Arquilla, John and Ronfeldt, David, (1993), "Cyberwar is Coming", Comparative Strategy, Taylor & Francis, Vol 12, (2), pp. 141-165.
4. Benefits of e-Government, Asia-Pacific e-Government Portal, Last modified 2004, http://egovaspac.apdip.net/topics/benefits/
5. Clarke, Roger, (1996), "Information Technology & Cyberspace: Their Impact on Rights and Liberties", Mietta's, The Australian National University, Melbourne.
6. Copeland, E., Thomas, (2000) "The Information Revolution and National Security", Strategic Studies Institute, U.S. Army War College.
7. CPME guidelines for Telemedicine, Standing Committee of European Doctors, 2002, http://cpme.dyndns.org:591/database/Telemedecine_2002.pdf .
8. Computer Crime definition, http://www.webopedia.com/TERM/C/cyber_crime.html, Consulted of May 03 2011
9. E-Government guideline, The World Bank, http://siteresources.worldbank.org/INTEGOVERNMENT/Resources/e-Gov_guideline.pdf
10. E-Government Handbook, CDT/infoDev, http://www.cdt.org/egov/handbook/
11. Forno, F.R. (1998) "Hidden threats and vulnerabilities to information systems at the dawn of a new century", Emergency Net News, 11/22, http://www. emergency. com/techthrt.htm
12. Freeh, J.L. (1998) "Threats to US national security: Congressional statement", FBI, January 28, http://www.fbi.gov/pressrm/congress/congress98/threats.htm
13. Guice, J., Duffy, R. (2000), "The future of the internet in science", USRA Research Institute for Advanced Computer Science, NASA Ames Research Center, USA, http://ase.arc.nasa.gov/publications/pdf
14. Horrigan B. J., (2004) "How Americans Get in Touch With Government", Pew Interne&American Life Project, www.pewinternet.org
15. Ottis, Rain, and Lorents, Peeter (2010) "Cyberspace: Definition and Implications", In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, pp 267-270.
16. Petrović R. S., (1999) "Globalno informaciono ratovanje", Zbornik radova (CD-ROM), YU INFO'99, Kopaonik.
17. Petrović R. S., (2001) "Neki aspekti nacionalne bezbednosti u informacionom dobu, Nauka, Tehnika, Bezbednost (NTB)", Rad po pozivu, UDC: 681.324; 65.012.8, Godina XI, Broj 1, str. 7-27.
18. Schudel, Gregg, and Wood, Bradley, (2000), "MODELING BEHAVIOR OF THE CYBER-TERRORIST", In Proceedings of Proceedings of a Workshop "Research on Mitigating the Insider Threat to Information Systems - #2", RAND Corporation.
19. Wills, David, and Bunn, Sarah, (2006) "Computer Crime", The Parliamentary Office of Science and Technology, www.parliament.uk/parliamentary_offices/post/pubs2006.cfm