CYBER TERRORISM – A GLOBAL THREAT TO SOCIAL ORDER

Žaklina Spalević[1],
Miloš Ilić[2]
Željko Spalević[3]

[1]Faculty of Tourism and Hospitality Management,
Singidunum University,
Belgrade, Serbia
[2]Faculty of Technical sciences,
University of Pristina,
Kosovska Mitrovca, Serbia
[3]University Donja Gorica,
Podgorica, Montenegro

Abstract:

Over recent decades, development has been based on the development of information and communication technologies. The Internet, one of the most widely spread technologies today, is used by individuals, companies, government and different government agencies. The widespread use of the Internet has contributed to the amount of data and information being shared. Thus, this medium has become a field of interest for different types of attacks. Cyber terrorism, one of the more frequent types of attacks, is based on the use of the Internet, and information and communication technology. All attacks are carried out against the security of the attacked country and its inhabitants. Cyber terrorism represents the greatest threat to national and international security since the creation of nuclear weapons. The paper provides an overview of registered cyber-attacks, with special emphasis on cyber- attacks registered in the Republic of Serbia and neighboring countries. It also provides a comparison of legal regulations which sanction the illegal activities of Internet users, especially activities aimed at disrupting security of states and their citizens.

Keywords:

Cyber-attacks, cyber-crime, ISIS, global network.

1. INTRODUCTION

There is no country in the world that does not have problems with some kind of terrorism threats and attacks. Today's mankind is based on the use of information and communication technologies (ICT). People all over the world use different computer based technologies. In many cases, human life and work cannot be imagined without daily use of computers and the Internet access. Internet users communicate by means of Internet technologies and different kinds of messengers. Communication via the Internet is especially important for people living in different countries. Different Internet protocols provide security and anonymity for all Internet users. Beside online communication, Internet users can share different kind of information, different files, and can exchange ideas and find things they are interested in. On the one hand, Internet technology provides users with all basic human rights. On the other hand, they need to respect obligations and policies of the use of Internet services [1]. Daily use of public and government Internet services, social networks and other services for data exchange provide great opportunities for the abuse of such

Correspondence:
Žaklina Spalević

e-mail:
zspalevic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2017-121-127

services. The proof of ICT wide spread is the fact that the functioning of most contemporary systems is based on ICT technologies. Power plants, water treatment plants, heating plants, air traffic control are just some examples of the systems where computers have complete control over all processes.

The extensive use of computer based systems and computer networks in different areas of human life and work has created open space for terrorist attacks. Terrorist can now attack different targets without their physical presence through the use of network services. In many cases these targets could not be attacked with conventional forms of attack. Some of them are national defense systems, nuclear plants, air traffic control systems, and systems for control of toxic waste.

In many researches the number of cyber attacks in technologically developed countries is compared to the number of cyber attacks in the countries that are not technologically developed. Particularly interesting fact is that the number of attacks in technologically developed countries is greater than one in the technically underdeveloped countries. Computer and network infrastructure in technologically developed countries is more vulnerable to cyber attacks.

Cyber terrorism represents the terrorist activity in cyberspace. This category includes all unlawful attacks on computer systems, computer networks and information owned by both individuals and governments. A cyber attack should result in violence against people or property or should generate fear among people in order to be characterized as cyber terrorism. As with traditional terroristic attacks, the main purpose of cyber attacks is human loss, the infliction of injury, material and economic damage to personal property. Attacks on critical government and military infrastructures could be characterized as cyber terrorism. [2].

The goal of this paper is to provide basic information for readers about cyber terrorism activities. The paper gives an overview of registered cyber attacks in Serbia and aboard. The paper analyzes the ways in which the attacks are carried out as well as the mechanisms of defense, from the technical and legal perspective.

The first section describes differences between physical and cyber terrorism. This section provides an overview of the advantages of cyber terrorism against physical terrorism in terms of the execution of terrorist acts. The second section represents some of the registered cyber attacks all over the world. Some of them can be classified simply as hacking, but some of them are more serious than that. In the third section cyber attacks registered in Serbia and former Yugoslav republics are being summarized. The fourth section describes technical and legal aspects needed for successful fight against cyber terrorism, while the fifth section summarizes main conclusions.

2. CYBER TERRORISM

Cyber attacks are just one of the possible Internet abuses that have a terrorist background. Six overlapping categories of Internet terrorist abuses are: propaganda, financing, training, planning, execution, and cyber attacks.

In general, a cyber attack represents the use of computer networks in order to attack selected targets. The purpose of these attacks is to prevent proper functioning of targets. Most often, targets are computer systems, servers or network infrastructure. Cyber attacks are based on hacking, computer viruses and malwares, flooding, etc. From the aspect of computer network security, each unauthorized or malicious access to the computer network can be classified as a cyber attack. Malware is computer software designed to gain access, compromise the confidentiality, availability or damage a computer without their owner's knowledge. Attackers secretly feed malicious software into the attacked computer programs or systems in different ways in order to achieve their goals. In flooding attacks central authentication servers of an organization are loaded with a large number of multiple simultaneous authentication requests. The purpose of this attack is server overloading for which Denial of Services (DoS) or Distributed Denial of Services (DDoS) attacks are used. In DoS attack, attackers use one computer and one internet connection in order to flood a server with packets. Packages are TCP or UDP. In order to perform DDoS attacks, computers and many connections are utilized. This is the main difference between DoS and DDoS attacks. Computers that are in use in DDoS attacks are often distributed around the whole world. In many cases these computers are abducted, and such network is known as a botnet [3].

From the perspective of execution, cyber attacks and traditional terroristic attacks can be observed as separate types of crime. From the perspective of perpetrators, these attacks are carried out by the same types of criminals, terrorist activists, and for the same reasons. Some advantages of cyber attacks over traditional terrorist attacks from the perspective of the perpetrators are listed below [2, 4]:

- Organization and execution of cyber attacks require less money than traditional terrorist attacks. From the perspective of equipment, terrorists must possess personal computer and an online connection. As a substitute for weapons and explosives, terrorists use computer viruses that they deliver via telephone lines, or Internet connections.

- Cyber terrorism perpetrators remain anonymous, which is not the case with traditional terrorism perpetrators. In cyberspace terrorists present themselves as regular Internet users. They use false nicknames for log on details or they log on as unidentified guest users. This kind of web portal access mask terrorists' real identity, and makes tracking almost impossible. Besides online anonymity, there are no physical obstacles in cyberspace that terrorist need to overcome. For example, terrorist do not need to cross borders in order to attack targets in other countries.
- Besides anonymity, the use of computer and Internet provide mobility for the attackers. Based on this, cyber attacks can be performed from anywhere in the world. Mobility provides additional level of security because the attacks can be performed within jurisdictions where the consequences of these actions cannot be addressed by the criminal justice system.
- Attackers are also able to extract far more data digitally than it would ever be possible in the physical world. For example, one gigabyte of data is approximately 4,500 paperback books. Hackers can extract all data by using a computer system within a minute.
- The number of potential targets is much larger and more diverse. Targets of cyber-attacks can be computers and computer networks owned by individuals, government agencies, different companies and corporations, private and government airlines, etc. The large number of computer based systems and computer based services in all aspects of human life and work guarantee that terrorists can find anomalies in the system that can be used as the key points for attacks. The fact that computers coordinate the work of critical facilities shows that it is impossible to eliminate all shortcomings. For example, some of the critical facilities can be electric power grids, emergency services, airline services, nuclear plants, etc.
- Cyber terrorism can be conducted remotely. In practice it means that cyber terrorism requires less people, physical and psychological training for attackers, and less money for travel than traditional forms of terrorism. This type of organization carries additional benefits such as more convenient ways to recruit and retain followers.
- Cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods. The reason for this is that cyber attacks provide greater media coverage in order to spread panic and fear, which is the main goal of many attacks.
- An attack may have much greater consequences than the same one carried out by traditional methods. For example, a traditional bank robber may only be able to hit one or two banks a week, while a cyber attack can target hudreds or even thousands of sites at one go.
- Attacks are conducted at machine speed. A terrorist hacker can write a piece of code that can target multiple sites in minutes. Besides, targeted sites can be located on the servers in different countries. Such attacks cannot be possible in traditional forms of terrorism.
- There is another aspect of cyber threat to be considered - the public and media perception of cyber crime. When large financial institutions have been hacked, the media have often apportioned blame to the organizations rather than criminals. This would not be the case in a physical bank robbery.

3. EXAMPLES OF CYBER ATTACKS

In February 2000, cyber terrorists attacked the websites of Amazon.com, e-Bay, Yahoo, and other renowned companies. The web sites were under the DoS attacks for couple of hours. After 2000, DoS attacks were registered in 2002, when thirteen root servers around the world were attacked. The functionality of these servers was to provide road map for practically all Internet communications worldwide. Unlike the attack in 2000, when there was downtime of the servers and websites, the 2002 attack did not cause slowdowns or downtime of the servers.

In July 2009, the United States and South Korea were under a series of coordinated cyber attacks. The targets of these cyber-attacks were websites of major government, financial and news agencies. Registered DDoS based cyber attacks targeted a wide variety of important resources. Some of them were banks, news websites, electronic government services, etc. During the attack, the access to these services was difficult or users were not able to get important information [5]. The number of hijacked computers for the purpose of this DDoS attack included 50,000, 20,000 and 166,000 computers from Symantec's Security Technology Response Group, National Intelligence Service and Vietnamese computer security researchers respectively. Such a number of hijacked computers are a testament to how serious these attacks can be.

In 2012, a modular computer malware named Skywiper or Flamer was used in attacks on computer systems in Middle East countries. Microsoft Windows was the installed operating system on the attacked computers. The malware spread through the computer systems and infected them via the usage of the local computer network or USB stick. In this attack over 1,000 machines were infected. Infected machines belonged to individuals, educational institutions, and government organizations. It was discovered that the malware was used for the purpose of espionage. Malware was design to record sound, including keyboard activity, screenshots, network traffic, even Skype conversations.

In 2010, Iranian nuclear facility in Natanz was infected by cyber worm named Stuxnet. The task of the worm was to destroy Tehran 1000 nuclear centrifuges. The worm spread through the network and infected more than 60,000 computers. Iran atomic program was compromised and set back for at least two years. The Iranian government believed that the attack was carried out by the Israeli and American computer experts hired by their governments, but there was no evidence for such an assertion.

In 2012, a number of cyber attacks were directed against computer networks in United States, countries in the Gulf Arabs (Qatar, Saudi Arabia), and Israel. In these attacks systems in a number of attacked banks were hacked. The Iranian government has been accused of carrying out the attack because it was believed that it was a response to the US cyber attack on Iran in 2010.

In 2007, a grocery retailer named Hannaford Bros was subjected to cyber attack. The attack was carried out by Albert Gonzales. In this attack more than 4.2 million credit and debit card numbers and other personal client data were stolen. A group of hackers led by Albert installed computer malware instead of databases on servers owned by the company.

After the attack, stolen account numbers and documents were auctioned at the Shadowcrew.com website. A year later, in 2008, the trusted payment processor Heartland Payment Systems lost more than 140 million dollars in damages incurred by the phishing attacks organized by Gonzales. In these attacks over 100 million individual card numbers were stolen. Heartland's motto and reputation were compromised too, which led to even greater consequences and losses. For these and other similar crimes Gonzales was found guilty and sentenced to 20 years in prison.

In 2006 and 2008, the International Olympic Committee, United Nations, 70 other businesses, defense contractors, and organizations were attacked. This attack was known as Operation Shady Rat, and it was assumed that the People's Republic of China was responsible.

In 2011, Playstation Network and Sony Online Entertainment were under cyber-attacks. In these attacks, 77 million user accounts were stolen. Private user data, credit and debit card information were stolen too. Total estimated damage was between one and two billion dollars. These two corporations were under attack for 24 days. During that period perpetrators were able to log on to the system and compromise data.

In 2004, computer networks in NASA, Lockheed Martin, Redstone Arsenal, Sandia National Laboratories, and several other facilities were attacked. These attacks were part of the cyber attack named "Titan Rain". Titan Rain has been one of the largest cyber attacks ever. Besides compromising the military system and confidential data, the attack had another dangerous side. Perpetrators created open space or so called backdoors for other hackers and espionage entities to infiltrate into these systems.

In 2007, the Estonian government websites were attacked in one of the most serious cyber attacks after Titan Rain. Attackers applied a number of different techniques in order to take down websites. Ping floods and botnets are just some of the applied techniques. The complexity of the used cyber methods pointed to the fact that the Russian government may be behind the attacks.

In 1999, a virus named Melissa, created 80 million dollars damage to companies in North America. The virus used Microsoft Outlook address book on infected computers to mass mail itself to the first fifty addresses. Besides, a virus created backdoor for other mass email worms including The Love Bug, Anna Kournikova, and MyDoom [6].

In 2000, the virus named ILoveYou shut down email accounts for millions of computers worldwide in a couple of hours. Total economic damage for the attacked business companies was between 6 and 10 billion dollars [7].

In 2000, the Japan's Metropolitan Police Department discovered that created software system for police vehicles tracking, including unmarked cars, was used by Aum

Shinryko cult. The cult had received classified tracking data on 115 vehicles since the beginning of espionage. The same system was built by Aum Shinryko cult as a subcontractor to another company. Further investigation found that the cult worked as a subcontractor to other firms. They developed various types of software for eighty Japanese companies and ten government agencies. The fact that they worked as subcontractors to other firms ensured their anonymity in organizations for which the software was created. Thus, all created software was compromised because there was possibility that the cult had installed Trojan horses into the system in order to launch or facilitate cyber terrorist attacks afterwards [2].

The United States military technicians discovered structural and engineering software, electronic models of a water dam, information on computer based water systems, nuclear power plants, and the U.S. and European stadiums in Qaeda computers which were found during the war in Afghanistan. The information shows that cyber space was used for research, communication and coordination of possible traditional attacks. These records show that it is possible to notice the connection between physical and cyber attacks.

4. REGISTERED CYBER-ATTACKS IN SERBIA AND FORMER YUGOSLAV REPUBLICS

Serbia is not immune to cyber threats, as any other co 0 on Serbian websites, including the website of the president of Serbia, and several ministries [8]. Most visible attacks are deface attacks, but there are also DoS attacks and DDoS attacks going on.

In 2014, the websites of the Serbian official institutions and the media were victims of DDoS attacks. Attacks were launched after the incident at a football match with Albania, and caused all but one Serbian news media website and associated servers to go offline [9]. The websites were unavailable for several hours. In those attacks, personal data of millions of the Serbian citizens were stolen from the database of Serbian Business Register Agency. Beside personal data, e- mails of the Interior Ministry officials were taken over [10].

In 2014, the DD4BC group of Bosnian hackers was discovered. They launched cyber attacks against a number of regional news portals, such as "buka.com," "istinito.com," "e- novine," "federalna.ba," "fena.co.ba," "kurir.rs", and "blic.net." First they launched short preliminary DDoS attacks, and then demanded payment in the virtual currency Bitcoin. If the victim refused, DD4BC would launch longer and more extensive DDoS attacks [11]. It was determined that the DD4BC group was also developing software intended for the exploitation of weaknesses of digital Bitcoin wallets in order to steal Bitcoins.

In 2017, the websites of the Montenegrin government and several state institutions, as well as some pro-government media, have been targeted and the cyber-attacks are on the increase [12]. Over 200 attacks on websites, state institutions, online fraud and misuse of personal accounts were reported in 2016, compared to only six attacks in 2012. The severity and sophistication of cyber-attacks affecting Montenegro during 2016 were reflected in the increased number of identified attacks on infrastructure and cyber espionage cases, as well as through phishing campaigns which targeted civil servants.

In 2012, the official NATO Croatia site was hacked and defaced by two members of TeaMp0isoN, TriCk, and Phantom. Besides defacing the site, they leaked logs dated between 2010 and 2012 to show that the breached server was being utilized. Their message written on the NATO website was seen by 20,000 people [13].

In 2015, the Croatian Telekom, one of leading providers of mobile telecommunication services in Croatia suffered a cyber attack. The problem was technically solved in ten hours, but during that period users were also affected. There were no data on how user data was compromised [14].

All of the mentioned examples testify to great threats posed by cyber terrorism. As we can see from the registered cyber attacks in Serbia and neighboring countries, severity of attacks is lower than in developed countries around the world. This can be discussed from two perspectives. First, our region has not been susceptible to cyber attacks, which is really encouraging. Second, our defense mechanisms are at a very low level so that the attacks remain unnoticed or companies do not report situations of possible cyber attacks in order to preserve the reputation.

5. TECHNICAL AND LEGAL ASPECTS OF CYBER SECURITY

Cybercrime has been present in the society for a long time in different forms. But, at today's level of development of the virtual dimension, it poses a constant and growing threat to the development and economic prosperity of every modern state. That is why countering cybercrime is also considered a priority cyber security area. Thus, it is necessary to define strategic goals to improve the efforts in countering this type of crime in the years to come.

There are two basic technical strategies for critical systems protection. The first strategy is defending the system from the internet risks while the system stays online. The second strategy is air gapping the system and the general networks, that is, a disconnection of such critical systems from the internet entirely by the authorities. A good example is the US government security mechanism named Einstein. This mechanism guards the US government computers and networks. It is designed to provide real time monitoring of possible intrusion in government computer network. In order to provide better security, this mechanism is connected with the Department of Homeland Security and the National Security Agency.

The adoption of the key documents such as strategies, action plans, conventions and other legal documents is the right approach and action framework of each country in order to solve this problem. The main goal of these documents is to provide enough information for different organizations on how to prevent cyber terrorism and deal with particular attacks. Fast technological development creates the gap between the uses of computer based systems and current law regulative in this area. Legal regulations should be created in order to cover new concepts such as cyber security and cyber crime. Some new concepts and objects are computer data, too. Computer data as new objects are not addressed by traditional legal regulations. Laws on technical developments are focused on physical objects around which daily life of industrial society is based. Many traditional laws applied in practice do not take into consideration importance of information and information technology that are associated with cyber crime and other forms of crimes which create electronic trace as evidence [15]. Many countries have elements of the legal enabling environment addressing cyber security and cybercrime, but these national legal frameworks vary widely in terms of the manner in which these issues are addressed. In today's globalized world, national, regional and international legal systems are intertwined [16]. They overlap between legal systems sometimes leading to collisions, and create jurisdictional gaps. In the cases of international cyber terrorism, gaps can lead to acquittal. In order to prevent the gaps each country need to harmonize cybercrime laws. The final goal is new law which can be based on single national approach or common legal acts identified in legal systems of other countries. This law, for example, can be expressed within a multilateral instrument.

6. CONCLUSION

Information and communication technologies incorporated in different infrastructures are essential for functioning. These computer based systems represent critical infrastructure sector suitable for different types of attacks. Recently, the cyber attacks have become a common threat to such systems. Well- organized attacks could produce huge damage. Damage can range from economic losses to human casualties.

In order to prevent cyber attacks or to reduce their severity, identification of critical communication and information infrastructure, and prescription of mandatory technical and organizational measures including procedures of reporting computer security incidents need to be carried out in a coordinated manner by central state bodies responsible for certain critical infrastructure sectors, critical infrastructure owners/operators and competent technical and security-related state authorities. Only if all institutions collaborated, the level of cyber security could be increased.

REFERENCES

[1] UNODC, “The use of Internet for terrorist purposes”, United Nations, New York, pp. 1-158, 2012.

[2] W. Gabriel, “Cyberterrirism? How real is the threat”, Special Report 119, United States Institute of peace, pp. 1-12, 2004.

[3] M. Lee, “DoS vs DDoS – what is the difference”, Security –faqs, Retrieved 15.12.2016, from: http://www.security-faqs.com/dos-vs-ddos- what-is-the-difference.html

[4] PGI Cyber, “What is the difference between cyber crime and traditional crime?”,Retrieved 12.01.2017, from: https://pgicyber.com/Newsand-Events/What-is-the-difference-between- cyber-crime-and-traditional-crime%E2%95%95

[5] Digital Attacks Map, “What is a DDos attack”, Retrieved 12.01.2017, from: http://www.digitalattackmap.com/understanding-ddos/

[6] U.S. Department of Justice, “Creator of Melissa Computer Virus Pleads Guilty to State and Federal Charges”, Press Release, 2002.

[7] L. Melanie, H. Lucy, “Google attack puts spotlight on China's "red" hackers”, Reuters - Technology news, 2010.

[8] M. Nikola, “Case of the cyber war: kosovo conflict”, Inspiration,org, Retrieved 15.02.2017, from: http://inspiratron.org/blog/2014/07/01/case- cyber-war-kosovo-conflict/

[9] W. Mike, "The cyber-attacks and fears of cyberwar to come", In news – draw your on conclusion, Retrieved 18.02.2017, from: https://inserbia.info/today/2014/10/the-cyber-attacks-and-fears-of-cyber- war-to-come/

[10] M. Ivana, "Serbia's efforts to respond to cyber security threats", OSCE, Retrieved 17.02.2017, from: http://www.osce.org/serbia/170361

[11] OCCRP, "Bosnia and Herzegovina: crackdown on 'cyber blackmail' group", Retrieved 20.02.2017, from: https://www.occrp.org/en/daily/4793-bosnia-and-herzegovina- crackdown-on-cyber-blackmail-group

[12] T. Dusica, "Montenegro on alert over new cyber attacks", BalkanInsight, Retrieved: 1.03.2017, from: http://www.balkaninsight.com/en/article/montenegro-govt-on-alert-over-new-cyber-attacks-02-21-2017

[13] K. Eduard, "Site of nato croatia hacked and defaced by teamp0ison", Softpedia, Retrieved 03.03.2017, from: http://news.softpedia.com/news/Site-of-NATO-Croatia-Hacked-and-Defaced-by-TeaMp0isoN-262429.shtml

[14] R. Ognjen, "Cyber risk alert croatia: ddos attack on ht (croatian telecom)-insurance solutions", Retrieved 05.03.2017, from: https://www.linkedin.com/pulse/cyber-risk-alert-croatia-ddos-attack-ht-croatian-ognjen-radulovic

[15] A. Artur, "Legal Aspects of Cybersecurity", Faculty of Law University of Copenhagen, 2014.

[16] F.P. David, "Overview of international legal issues and cyber terrorism", Study Group on Cybersecurity, Terrorism, and International Law, International Law Association.