Cyber Terrorism in Slovenia– Fact or Fiction

Igor BERNIK
University of Maribor, Faculty of Criminal Justice and Security
Ljubljana, SI-1000, Slovenia

and

Kaja PRISLAN
University of Maribor, Faculty of Criminal Justice and Security
Ljubljana, SI-1000, Slovenia

ABSTRACT

Article represents the cyber terrorism and the way in which the Slovenian organizations understand and manage it. Cyber terrorism in public is usually referred and is mostly mistaken for classic attacks on information systems. The cyber terrorism can with minimal effort and knowledge cause terrible consequences and threaten existence of every organization. Methods and techniques of such attacks do not differ from the operation of the classic information security threats. However, the terroristic attack strives to political and social changes in order to spread fear among general public. The most common attacks are pointed on information systems in critical infrastructure. The consequences of the terroristic attack on the organization’s information system are mostly economical damage, employees’ injuries or even death. The protection against such cyber threat is therefore necessary; however it depends on every individual organization. With results explanations, gathered with interviews in Slovenian organizations we are able to learn about problems of understanding cyber terrorism as a threat and to properly adjust to the changes.

Keywords: cyber terrorism, information security, risks, threats, managing the threats.

1. INTRODUCTION

An importance of the information and an ability of its access, transfer and operation have reached the level where one cannot imagine the management without using a computer or Internet. More the value of the computer infrastructure increases, higher is the value of damaging it. On the one hand, we face the financial consequences. Nevertheless, the psychological consequences of disconnecting the Internet and information systems can be even more damaging [1]. Namely, the computers control the systems of critical infrastructure, such as electricity supply, communication, air transport and financial services. Organizations use the computers for saving vital information, for instance, medical records, business plans or penalty records [2]. For that reason, they have to be aware of the most common terroristic attacks, and provide appropriate protection. Otherwise, a disclosure or a damage of the confidential data can lead the organizations into collapse.

Cyber terrorism is a carefully planned, politically motivated attack on information, computer system, programs and data [2]. In order to be able to classify it, it must be designed in a way to cause fear and influence the society as well as the authority [3]. Computers cannot directly kill or injure a person; however, indirect risks of physical damages and direct risks of economical damages are possible. It exist an option for computers to connect to other devices, which have a physical ability to cause a death or an injury. As we name/use computers as a weapon, we should take into consideration that their acts are indirect [2]. In spite of that, the consequences may be giant, even bigger than by the classic terroristic attack.

The most recognizable and the most common type of cyber terrorism is an attack on information system. The main aim of the attack is changing or damaging the contents of the electronic files, computer systems or other material. The other type of the terroristic attacks is pointed to destruction or damaging of critical information infrastructure. They include the attacks on heavy equipment and software. By those attacks the side effect is data damaging. Finally, the third type of cyber terrorism uses the Internet and information systems for an execution of a classical terroristic attack [4].

In public, the most common and the simplest attacks are named as terrorism because the methods and technique of cyber terrorism do not differ from the other malicious attacks on the information system. However, a difference exists: a motivation, which leads on the one hand classical hackers and on the other hand terrorists who uses the Internet for achieving their aims. They both strive for the same consequences – political and social changes. Nevertheless, the hackers and crackers take advantage of security gaps in the information systems due to various reasons. The most common reasons are wish for proving and searching and warning of the security gaps. Sometimes they operate on order, and at this point, the hackers and the terrorists may come into contact with each other. That is possible when the terrorist are ready to offer the hackers an adequate amount of financial sources for an execution of the cyber attack on the information system of the government institutions and giant corporations, or on the system of critical infrastructure. In this case, the hackers’ aims are not political, but financial [5].

The experts in this field of study still do not agree on the damage which may be caused by cyber terrorism, despite the fact that cyber terrorism threat exists as long as the internet. The most common consequence of the attack is economical damage; however, in appropriate conditions, when the attack is focused on the critical infrastructure that is important for people, the consequences can indirectly be seen in injuries or deaths of people. The terrorists use the online services for other needs as
well, such as planning, coordinating, advertising, recruiting, propaganda and collecting financial means. However, the direct attacks on information systems are more and more frequent due to technology development. It is concerning fact that the internet is used by more than 26% of world population [6], and few millions of it misuses its abilities for malicious acts. Managing cyber terrorism is therefore vital for protection of financial and information material in organizations at a micro and macro country level. From that we can gather that cyber terrorism represents modern security threat to every information system. The most exposed and vulnerable spots of those systems are information and communications, electricity network, gas and oil (storage, transport, production), banking and finance, transport, water providing systems and government services. In order to protect those spots against the attacks, they must be as physically moved from Internet and information systems as possible. In addition, people who are managing such systems must be qualified accordingly [7]. The organizations as well as countries are responsible for the countermeasures. However, they have to take into consideration that classical antiterrorist measures against modern type of terrorism do not bring a success [8]. New approaches must be taken over, and in order to achieve that, the enemy must be known thoroughly. The organizations must be especially aware of those facts because the private business centre represents 85% of the Internet [9]. The system is secure as much as its weakest part secure is. The weak protected companies, which are not able to manage the attack, threaten the entire security and efforts of country and global community. The organizations therefore must not avoid the system analysis and the risk management, in order to protect themselves sufficiently. The process of the risk management fundamentally does not differ from the classical one. The consequences are the most important factor which decides whether the system will provide protection or not, and in what way will it provide it. The aim of providing as sufficient information security as possible (the complete security is impossible) pushes the organizations into exact research of their infrastructure and threats. It depends on each organization if it considers cyber terrorism as a threat, and also for which way of managing the risks the organization decides.

Cyber terrorism is relatively unknown phenomenon due to its modernity. In order to achieve a sufficient protection against the future threats, the security should be provided immediately. Namely, the prevention is better than cure. With help of directed interviews among 20 different Slovenian organizations (smaller, bigger, in public and private sector) we tried to research what is the level of understanding this type of threat in commercial environment. The purpose of the research is to do an overview and comparison between the organizations about their understanding of cyber terrorism, the protection ways, measures and awareness of the future threats.

2. RESULTS

Results presented bellow were gathered with the interviews in 20 Slovenian organizations from different work fields but with 15 and up to 50 employees (middle size companies in Slovenia) in the second part of 2010. By doing the research of the understanding of cyber terrorism, a half of the questioned organizations agree that an aim of the attack on the information system is stealing and damaging of data. However, they did not consider the main component, which actually defines the terrorism: political motivation for causing fear. Only 15% companies understood the point of the phenomenon. This information is alarming due to an increase of the threat and its ability to cause enormous business damage. There are different reasons for the wrong understanding of cyber terrorism: one of them is probably a consequence of lack of experience by managing such problems; the next problem is lack of knowledge and awareness about such computer criminal.

Two thirds of the questioned organizations consider cyber terrorism the same as the other threats and that is logical due to the incomprehension of it. However, the organizations that understand the point of cyber terrorism consider it as unimportant. At the moment, cyber terrorism does not represent a topical issue to information systems, nevertheless, we believe that in the future is going to be more often and more dangerous. The organizations should therefore draw attention to education in the field of understanding and security against terroristic threat.

About 64% of organizations understand protection against cyber terrorism the same as protection against other threats because they equate it with other threats. The security is therefore weak: they do not use any special protection mechanisms, which means they make use of general security techniques. That actually makes sense because the terrorists in a cyber space use the same techniques and methods as classic terrorists. Therefore, the security against hackers’ attacks is useful for protection against terrorists. However, the equality with other threats is dangerous, so the organizations should be more aware of nature and power of such phenomenon. Better understanding of power of cyber terrorism could improve the protection, and could aid in abolition of consequences.

Even though the most of organizations do not consider cyber terrorism as a serious threat, they share the opinion that the terrorists will more and more often use the advantages of information and internet services for achieving political aims. That means that organizations are aware of changes in information environment. Information technology is an integrated part of modern society, and the organization cannot successfully operate and be competitive without it. The enemies are aware of it, and with adequate knowledge and minimal effort they can break through protection barriers and disable information systems due to weak protection. Awareness of danger growth of such threat confirms a high level of security culture.

More than a half of questioned organizations believe that the future threats are going to be more dangerous. We agree on it because the danger of the threats is going to increase more and more due to development of structure and methods of the threats. The threats are therefore going to threaten existence, business and operation of information systems in the future. However, it does not mean necessarily that the organizations are going to be more threatened. Namely, as the threats are changing and developing the protection against them is also getting better. The only difference is that development of threats does not depend on organizations. The threats develop together with changes in international, social and technological environment, while the protection of information systems depends completely on will of organizations. The organizations must take care that the jeopardy and vulnerability of their information systems do not increase but adjust to the future protection threats.

Much can be done for increasing of information security. 47% of the organizations focus mostly on education and awareness of the users of data and systems, and on the employees who operate with them as well. Prevention is the most important measure for a long-term abolition of security problems. Other essential
measures are following the news in the field of threat development, and updating the mechanisms of protection. Introducing those into information structure means the increase of level of protection and security.

The organizations believe that they can avoid cyber terrorism in the same way as other threats. However, in our opinion, it is hard to avoid those threats in such way. The users and the employees can only bring vulnerability of information systems to the lowest possible level, and that is all what one can do – we cannot completely avoid it. The only way to avoid it is to not have information system. Namely, once we got it, there are always weaknesses, which can be misused by people with adequate knowledge and motivation, in spite of all protections and precautions.

3. CONCLUSION

Cyber terrorism as one of the modern threats to information systems is in public mostly mistaken for classical computer criminal due to their similarity in form and way of operation. The results of the research among Slovenian organizations in the field of information security confirm this fact. Most of the organizations equate the cyber threat with other threats, and provide the same protection for both types. Protection against the terroristic threat therefore does not differ from protection against the other threats due to the same risk management in both cases. Damage caused by the terroristic attack on information system would probably draw more attention to such type of terrorism; however, the organizations have not been targets of such threats yet, and therefore it is hard to evaluate the possible damage. In the future, the organizations expect more powerful activity of terrorists in information and communication environment due to escalation of dependence on information technology and disability to operate without online and computer services. For that reason, the organizations draw the most attention to preventive measures. Despite weak understanding of terrorism in virtual world, we believe the organizations are working out well by achieving a sufficient level of awareness and preparation to face the latest (virtual) threat to information security.

Unfortunately, dependence of organizations on information technology is too strong, so we cannot avoid the threat. The most we could do is to prepare the best possible renewal procedure in the case of the attack, and to make all users of system and its managers aware of the possible threats. In light of this, cyber terrorism is a serious threat that must be taken into account to provide a comprehensive information security. To date, there was no known successful attack on information infrastructure that could be defined as a complete cyber terrorist attack. However, we need to take it seriously and be prepared to threat of cyber terrorism attack. “Looking at the history of cyber crime it has been shown that there is definitely a need for more protection. Knowing that cyber terrorism exists is the first step to a solution [10]”. To conclude, cyber terrorism is a modern and therefore unknown phenomenon.

4. REFERENCES