NATIONAL UNIVERSITY OF PUBLIC SERVICE

DOCTORAL SCHOOL OF MILITARY ENGINEERING

Author's summary

Zoltán István Papp

METHODS AND POTENTIAL MEANS OF CYBER-TERRORISM AND THE ALTERNATIVES OF DEFENCE AGAINST THEM

Doctoral (PhD) thesis

Consultant:

Prof. Dr. Col. Eng. László Kovács Ph.D.

professor

Budapest, 2018.

Identification of the scientific problem

Information technology infrastructures have a major role in the high-quality operation of information societies, which makes them a target of many malicious and harmful activities carried out with versatile methods by different attackers with various motivations. In terms of the threat posed to modern societies, cyber-terrorism rises above even these activities because, similarly to "conventional" terrorism, it has the widest repertoire of means and methods. Furthermore, the opportunities provided by cyberspace allow cyber-terrorists to conduct their illegal activities with a considerable degree of anonymity and independently of geographical space.

In order to achieve certain objectives and based on various reasons, information infrastructures can be attacked by governmental organs and organizations (military units, intelligence services) outside the alliance system of the given country, which are specifically established for such purposes and operate using professional devices and methods. The efficiency of such offensive activities may largely be increased by the fact that governmental organizations tend to have practically unlimited human and financial resources and often possess technical, technological and personal databases as well. Another efficiency-increasing factor is that the government can create such a legal and law enforcement environment that supports these activities.

In addition to the threats originating from organizations of counter-interested countries, information infrastructure may also be targeted maliciously and illegally by individuals, irregular organizations or terrorist groups operating in cyberspace in an effort to block its services and/or obtain, destroy or manipulate the information stored therein.

Beside the regulatory environment requiring such offensive activities to be sanctioned, potential perpetrators are also hindered by the fact that most of the appropriate devices are typically deemed as military technology, which means that they either cannot practically be procured, or only through a substantial expenditure. Depending on the depth of the perpetrators' motivation however, they have less and less legal or moral concerns, so they ignore the regulatory bans, they do not appropriately consider the legal ramifications of their actions, therefore they definitely carry out the illegal acts against information infrastructures, using all available information and means to achieve their goals.

There are several circumstances to aid potential perpetrators since the information systems used by modern information societies contain a mass of information, services and other

opportunities that can be utilized by way of investing certain amounts of time and funds. Firstly, information infrastructures are not only vulnerable through the content of the information stored therein but also through other features and parameters. Secondly, attackers may obtain substantial and useful information regarding the affected infrastructure, the applied hardware and technologies as well as the employed personnel. Furthermore, they can gain supporters for their cause, ensure the financial means while they may also acquire and learn the know-how and methodology indispensable for any successful attack.

Such illegal activities are further aided by the fact that there are many physical and logical tools and methods which can enable attackers to interfere with the operation of information infrastructures. The commerce and possession of some physical tools are forbidden by law but many of them can be created by using commercially available parts or can be substituted by modifying certain other equipment that are commercially available.
As far as logical tools (malicious codes) are concerned, attackers of information infrastructures can more easily use them than physical tools. The device of implementation, i.e., the computer is available for anyone; the existence of the logical tools belonging to this category is not detectable in the physical sphere; their possession is practically uncontrollable. Moreover, while their development requires in-depth knowledge, their application does not. Many programmes are already available in a "ready-to-use" form, requiring nothing more than the identification of a target. Also, the malicious codes constructible from various tool-kits and other available or obtainable vulnerabilities may also pose serious threats to information infrastructures.

Considering the role of information infrastructures in modern information societies, we must constantly ensure the acquisition, flow and use of information as well as the permanent functioning and necessary conditions of the systems, equipment and transmission channels used for such operations. However, there are many factors, within or outside the operators' sphere of influence, which could have an impact on permanent operational security and general safety.
It is difficult to protect information infrastructures because there are several circumstances either unknown or not fully taken into consideration until they actually arise, or which did not even exist at the time when the infrastructure was configured. So the developers of defensive measures and the designers of protective sub-systems must apply utmost caution to predict and foresee any potential threats and dangers in terms of each security area, which is

impossible without an extensive knowledge of the current situation as well as a correct forecast of expectable trends.

Maintaining security is a major challenge both in the physical and the cyberspace. The circumstances affecting security are highly complex. There may either be internal and external circumstances which can impact the security status of the information infrastructure but the phenomenon that negatively affects security may arise as a co-efficient result of external and internal factors.

In addition to the operators, the secure functioning of infrastructures is also in the interest of the state representing the citizens of a modern information society, for which the relevant bodies, organizations and authorities have a responsibility. In the defence area, the relevant parties already cooperate or are forced to cooperate but the different interests and opportunities (or the lack thereof) of the parties do not affect towards the rapid development of an ideal situation.

In light of the above, we need the means of science in order to identify the correlations and interferences of the above factors. Further scientific research is needed to investigate what conditions and effects are instrumental in members of the information society taking to cyber-terrorism; what methods and tools they may apply to attack which features of the information managed in information infrastructures; and we also need to look into what opportunities or new methods infrastructure operators and/or states can have in terms of defence and what circumstances actually affect against security.

Hypotheses

Beyond the contents of the generally defined information managed in information infrastructures or the temporary information related to the processing thereof, this information has other characteristics and features which cyber-terrorists can manipulate in order to hinder the standard operation of infrastructures and the ongoing information technology processes.

The social impacts on the members of the information society, the opportunities arising for them in cyberspace, the available tools and the accessible information allow individuals to become cyber-terrorists - under a particular constellation of relevant effects. On the other

hand, these social impacts typically determine what type of infrastructure the particular individuals will attack, for what purpose and by what method.

In connection with the scheme of complex information security, operators and state authorities may introduce such new aspects and work processes that can increase the security level of information infrastructures.

Studying the characteristics related to the operation and protection of information infrastructure may enable us to reveal such correlations and risks in our own internal processes and/or in relation with other connected infrastructures that can potentially impact our security situation. We definitely need to constantly monitoring the current status and potential changes of these factors in order for us to prevent any negative changes in terms of the security situation.

Research objectives

To explore such characteristic features of the information the manipulation of which allows cyber-terrorists to achieve a dysfunction in the operation of information infrastructure and/or user activity.

To determine how the level of commitment, the "willingness to execute" illegal acts in cyberspace, i.e., cyber-attacks, changes by perpetrator and how it relates to the general or perceived social processes and background of the particular individual.

To determine whether the investigation of social processes and backgrounds is justified in cases where the threat and offensive potential of a certain social circle or group needs to be assessed, and/or whether a social analysis can be applied indirectly, i.e., if we could assess what social groups may pose the largest threat to a particular function of information infrastructure – based on the qualifications, extreme political views and/or financial status of the individuals belonging to such groups.

To categorize the activities and different methods defined within the framework of cyber-terrorism, and to categorize physical and logical tools potentially used by cyber-terrorists.

To define measures to be executed by the state and the operators in order to prevent and detect threats; to identify potential areas of cooperation and reveal any factors affecting against a closer cooperation, constant operation, security and protection.

To develop such methods that could allow both the operators and the state to increase the efficiency of protective measures or to reduce risks.

Research methods

The preliminary overview of the literature on the chosen subject already revealed that the assessment of the various aspects of cyber-terrorism and the defence against it would require a combinative application of several research methods.

In my research work, I studied the international and Hungarian literature and legal documents as well as the electronic and printed outputs of mainstream media, which had an utmost importance in extending my view, cross-checking information obtained from other sources as well as in terms of case studies.

I collected data presented by experts in scientific conferences and professional meetings (workshops, focus group discussions), which constantly formed the orientation of my research activity.

In the course of my work, I analyzed and evaluated the information I gained with regard to cyber-terrorism, and sought scientific answers concerning the acquired experience and conclusions.

My analytical work also covered the information and experience that arose during the cooperation with Hungarian and foreign partner organizations – in order to confirm or disprove them by comparing them against the relevant statements and conclusions indicated in the literature.

I made structured interviews with individuals employed at different executive levels in the various areas of information infrastructure operation, and analyzed, evaluated and used their input and information in my research work. I also conducted interviews with individuals

involved in different criminal acts carried out in cyberspace, and their input and information were used in my research work as well.

Having synthesized and evaluated the information gained through the research methods described above, I laid out my partial conclusions, which then led me to answering the scientific problem.

Brief chapter-by-chapter description of the conducted analysis

CHAPTER I

Information and the information society

In the first chapter I gave an overview of the approaches bringing about the different definitions of information society as provided by the different branches of science, thus identifying the criteria that define this new form of society. I looked into how the information society transforms the relations among the members of such society as well as which phenomena may be evaluated as a threat to the information society and how they exercise their effect. I studied cyberspace as the medium where this new form of society gains its function. I analyzed the differences between the civil and military approaches to cyberspace.

I investigated the nature of information and why it has such an utmost significance for modern societies. In the context of that work, I looked into the key qualitative criteria for the practical utilization of information and how they may influence the leadership cycle.

I reviewed the meanings, types and functions of the information infrastructures hosting cyberspace as well as the features of criticality. Moreover, I investigated the potential threats to critical information infrastructures, with special regard to the threats related to malicious and/or harmful acts and activities. I analyzed the perpetrators of these acts along with their motivations and the characteristic features of such acts.

CHAPTER II

Cyber-terrorism

I studied the phenomenon, goals, types and legal definitions of terrorism, along with the factors that may influence the different legal definitions in the different countries, making

their mark on the definition of terror in the particular country. I analyzed the potential parallelisms between terrorism and asymmetric warfare.

Studying cyber-terrorism that inevitably appears along with the development of technology and the information society, I reviewed the various definitions published in the literature. Having drawn my conclusions and evaluating my own experience, I laid out a definition of cyber-terrorism in a way that, in my opinion, best describes this phenomenon.

I investigated the social effects, circumstances and life situations that may potentially lead to members of the information society become cyber-terrorists. I analyzed the life situations of individuals belonging to different castes of cyber-terrorists as well as the factors affecting the development of such castes. In the context above, I have identified several circumstances that may be instrumental in a member of the society becoming a perpetrator of terrorist acts committed in cyberspace.

CHAPTER III
The tools of cyber-terrorism

Based on the Hungarian legal regulation, I classified the potential methods of cyber-terrorism into three parts: support; funding and logistics; implementation.

Looking into the support methods in terms of the relations between terrorism and the media, I studied the propaganda activities carried out in cyberspace by terrorist groups and I focused on two methods. Regarding the methods to spread ideology, I investigated the special characteristic features helping terrorists to make their messages accessible through cyberspace to a wide group of the information society. Analyzing the activities related to the recruitment of supporters, I pointed out the ways in which the quality of these goes significantly beyond spreading ideology.

In the funding and logistic methods section, I researched the activities that allow cyber-terrorist groups to maintain their organization, operability, action readiness and fundability. Investigating the methods of communication and information sharing, I identified the options of keeping contact which the affected parties can safely use in the course of their illegal activities. Concerning the collection of resources and using services, I searched for the

solutions that may potentially help them prepare for the terrorist acts and to create the necessary conditions. Looking into the methods of raising funds, I studied the activities enabling terrorist groups to obtain financial resources.

Regarding the methods of attack, I investigated the activities that are suitable for representing the philosophy of terrorism in the information society. I collected the methods belonging to identification of potential targets and gathering information about them; and analyzed their efficiency. Having studied the activities related to attacking the targets, I categorized them and investigated the phenomenon of interdependence of these activities.

CHAPTER IV

The tools of cyber-terrorism

In this chapter I studied the physical and logical tools, their relevant applicability and efficiency, which cyber-terrorists may use against information infrastructures and their acquisition is not blocked by insurmountable obstacles. I explored the differences between professional and non-professional tools.

In terms of the physical tools, I looked for potential methods, focusing on electronic counter-activities with special regard to equipment related to electronic destruction.

Looking into logistical tools, I studied the arguments for their applicability and analyzed the anomalies related to their potential use and
reviewed the types of attacks that could be suitable for implementing terrorist attacks against information infrastructures.

CHAPTER V

Defence solutions against cyber-terrorism

I studied the components of the threats in terms of information infrastructures, as well as what effects they may induce in the various status indicators.

Reviewing the professional areas of complex information security, I investigated the type of threats potentially posed by cyber-terrorism to these areas. Having reviewed the specific

features of each professional area, I concluded that it was necessary to enhance defence measures with national security defence, asymmetry analysis as well as a map of operational and security interdependence.

Recognizing the importance of prevention among the potential defence solutions, I looked for the potential methods for operators and state actors to contribute to improving the security of information infrastructures.

Summary and conclusions

Studying terrorism as a phenomenon, we can draw the conclusion that its methodology and objective have not changed significantly ever since its first appearance. The purpose of randomly applied violence in the name of a particular ideology has always been to oppress and keep certain social groups in fear and insecurity as well as physically destroy the members of such groups. This fundamental objective has hardly changed over time at all, so the statement applies to the present as well. However, the phenomenon has one component which has constantly improved from era to era, and that is the tools applied. The achievements, technological levels and scientific results have always been reflected in it: the current cutting-edge technology always appeared in terrorism soon after it was invented and developed.

Cyberspace was created as a result of the developing information processes, the increasingly modern and efficient hosting and supporting infrastructures and their subsequent globalization. The new technologies and technical solutions appearing in the information infrastructures aided the information processes and when they exceeded a critical size, an infinitely high number of social functions were organized around them and their services, leading to the term “information society”. This society depends upon the constant acquisition, flow and availability of the sufficient amount of information not only for its growth but also for its seamless operation.

The above statements also lead to the conclusion that, in order to achieve its goals, terrorism needs to “take root” in the information society as well: both by terrorists entering and integrating into this society themselves, using and abusing its opportunities and tools, and by conducting their activities against this society through disrupting its processes which allows them to accomplish their primary goal: to generate fear and insecurity. Therefore the

appearance of cyber-terrorism as the common set of terrorism and cyberspace is practically an inevitable consequence of technical-technological development.

We can also conclude that due to its special features, cyberspace may help certain members of the information society to become cyber-terrorists as long as the disposition to radicalize and the appropriate circumstances are present. Firstly, terrorist groups may conduct their propaganda and recruitment activities more easily in the cyberspace because geographical and state borders no longer pose an obstacle, they can easily differentiate and customize their messages based on the "needs" of their target groups and the expectations of their supporters, which significantly increases their efficiency as they can easily "find each other" with such supporters. Secondly, the execution of illegal cyber-activities takes place in a safe cocoon (often in the "warmth of the home"), so the perpetrators do not even approach the victim physically; there is no contact between them. Due to this circumstance, perpetrators experience their acts in a different (typically not in a negative) way, they remain psychologically unaware of the fact that they cause damage and harm and they put others in danger through their acts. This especially applies if they are unaware even of the illegal nature of their acts – due to ignorance and lack of information. Thirdly, logical attacks are committed by using a tool that is a "fundamental asset" of the information society, i.e., the computer which is accessible to anyone, and even physical attacks can be carried out by using tools that can be obtained, modified or created relatively easily. Fourthly, cyberspace provides several services and opportunities for terrorist groups to easily keep contact, fund their activities and execute their specific terror attacks as well. Furthermore, cyberspace provides excellent opportunities to remain anonymous and to hide digital paths, which allows perpetrators to constantly keep experimenting (even teaching themselves) and encourages "first triers" to execute their illegal acts. In light of the above, we can forecast that cyber-terrorism will keep making up an increasingly large share of terrorism – in line with the development of the information society.

Studying the tools of cyber-terrorism, we can predict with a high probability that the application of logical tools will form a significant part of terrorist acts as well as the attempts thereof. This is because the application of physical tools requires substantially more organization, background knowledge, feasibility data, financial expenditure and thus significantly more commitment than the application of logical tools. The application of logical tools is considerably easier for the vast majority of cyber-terrorists because the descriptions

and feasibility data of methods and the information on target vulnerability are readily available online. Meanwhile, the malicious codes themselves can also be obtained relatively easily (even in the form of toolkits) or the available ones can be transformed, "customized" or even developed and applied repeatedly or in parallel as long as the perpetrator possesses or obtains the relevant know-how. Furthermore, the possession and development of these tools is hardly detectable, so they can be applied in a safe and risk-free manner as long as the appropriate measures are taken.

Studying the process of becoming a cyber terrorist and the investigation into the methodology and capabilities of physical and logical tools can lead us to the conclusion that cyber-terrorists – in lack of professional tools and truly in-depth knowledge – currently cannot pose a systematic threat to information infrastructures by way of the widely available or constructible tools. However, they can cause detectable disruptions and relatively great damages locally or to certain sub-systems, which – although they may attract media attention – will not derail the global processes of the information society even if they may significantly affect certain social entities both financially and emotionally.

Nevertheless, the damage and/or disruption may be increased significantly if the cyber-terrorists find such security loopholes, asymmetries and interdependence relations which the affected parties (e.g., law enforcement agencies, business partners) were unaware of or failed to address.

The above statements lead to the conclusion that asymmetry and its various dimensions will pose an increasingly significant problem in terms of the active and passive protection of information infrastructure, the assessment and damage management of cyber-attacks and the identification of perpetrators. If the attackers can identify the weaknesses of the protective system, the interdependent relations, the potential areas of asymmetry and plan their acts accordingly, then they can pose extraordinary difficulties for the operation and protection of information infrastructures as well as the activities of the authorities wishing to fight them.

This also brings us to the need for a complex, universally solid defence. The applied defence system must guarantee the continuity of information infrastructure services and the security of the managed information upon the appearance of any circumstance considered during system design. However, the establishment of a defence system is not a one-time task but an activity involving constant monitoring, data collection, planning and development which must cover all aspects of security.

New scientific findings

1. Having summarized the experience and knowledge gathered through studying the illegal activities or series of acts committed in cyberspace in relation with terrorism, I created the definition of cyber-terrorism. The definition represents the unique feature that cyber-terrorism concurrently considers information infrastructures as the target and the means of execution.

2. Having synthesized the knowledge acquired by studying the cyber-activities of various terrorist groups and the acts specifically related to cyber-terrorism with my own experience, I categorized the methods of cyber-terrorism and described the activities belonging to these categories.

3. Regarding their information infrastructures, I suggest both the operators and the state organizations involved in defence and law enforcement to conduct an asymmetry analysis in order to improve their efficiency and productivity. Such analyses may reveal the factors and the various combinations thereof which may unexpectedly inhibit or weaken the prolificacy of responses to be given to various incidents and effects.

4. In order to explore the correlations lying in the operational and security circumstances of information infrastructures as well as the consequences of the different external-internal effects, I propose to introduce an operational and security map so that both the state actors involved in infrastructural defence and the operators could see the resultant of all the negative effects potentially impacting the various professional areas in the entire spectrum of complex information security.

Recommendations, practical applicability of the findings

I propose using the contents of the doctoral dissertation as education material for university undergraduate and graduate courses related to the information infrastructure, cyber-terrorism and certain professional areas.

I propose integrating the parts of the dissertation on the nature, methods and tools of cyber-terrorism into further education materials for law enforcement and national security personnel employed in this area.

I propose using the comments and recommendations laid out in the dissertation in the training and further training courses for experts of information security in information infrastructure.

I propose considering the conclusions of the dissertation for designing the complex defence of information infrastructures, developing operational strategies as well as the relevant legislation and regulatory environment.

List of publications on the topic of the thesis

- Zoltán Papp: RFID – Új technológia veszélyei: RFID és az elektronikus útlevél (”RFID – The risks of new technology: RFID and the electronic passport”), „Hadmérnök” Volume V, Issue 4, December 2010 - pp 248-254., ISSN 1788-1919
- Zoltán Papp: Irányított energiájú fegyverek veszélyei a kommunikációs hálózatokra (”Threats of directed-energy weapons to communication networks”), „Hadmérnök” Volume VI, Issue 4, December 2011 - pp 233-238., ISSN 1788-1919
- Zoltán Papp: Az információ támadása annak tulajdonságain keresztül (”Attacking information through its characteristic features”), „Hadmérnök” Volume VI, Issue 4, December 2011 - pp 224-232., ISSN 1788-1919
- Zoltán Papp: A helyzet-meghatározó rendszerek zavarása (”Jamming of positioning systems”), „Hadmérnök” Volume VII, Issue 1, March 2012 - pp 214-221., ISSN 1788-1919
- Zoltán Papp: A számítógép-hálózatok tűzfalainak támadása (”Attacking computer network firewalls”), „Hadmérnök” Volume VII, Issue 2, June 2012 - pp 335-341., ISSN 1788-1919

Zoltán Papp – Erik Pándi – András Kerti: A számítógép-hálózatok elleni támadások módszertana (”Methodology of attacks on computer networks”), “Communication 2009.” international professional scientific conference, October 14, 2009 - pp. 143-154. ZMNE Budapest, ISBN 978-963-7060-57-1

Zoltán Papp – Erik Pándi – Ákos Töreki: A fenyegetettség egyes aspektusai az információs infrastruktúrák tekintetében (”Certain aspects of vulnerability in terms of information

infrastructures"), "Communication 2009." international professional scientific conference, October 14, 2009, - pp. 155-163., ZMNE Budapest, ISBN 978-963-7060-57-1

- Zoltán Papp: Virtuális magánhálózati kapcsolatok ("Virtual Private Network connections"), „Hírvillám" Professional Scientific Journal of the Communications Faculty of Miklós Zrinyi National Defence University (ZMNE), Volume I, Issue 1, December 2010 - pp 156-162., ZMNE Budapest, ISSN 2061-9499
- Zoltán Papp: RFID – Új technológia veszélyei ("RFID – The risks of new technology"), „Hírvillám" Professional Scientific Journal of the Communications Faculty of Miklós Zrinyi National Defence University (ZMNE), Volume I, Issue 1, December 2010 - pp 271-275., ZMNE Budapest, ISSN 2061-9499

Zoltán Papp – Erik Pándi – Zsolt Dorkó: Információs rendszerek alkalmazási feltételeinek korlátozása ("Restrictions of the application criteria of information systems"), Study – 2010. – p. 92, ZMNE University Library, Budapest

- Zoltán Papp: Information terrorism, „Hadmérnök" Volume VIII, Issue 4, December 2013 - pp 217-222., ISSN 1788-1919
- Zoltán Papp: Professional areas of protection against information terrorism, „Hadmérnök" Volume IX, Issue 3, September 2014 - pp 207-213., ISSN 1788-1919

Professional and Scientific Curriculum Vitae

I completed my secondary education in Miksa Déri Industrial Secondary School of Szeged, Hungary, obtaining my A-level certificate and also my qualifications in general machinery and maintenance. During my secondary studies I successfully participated in national professional educational competitions of various levels.

Based on my school studies, I was enrolled as a student of the organization and information technology faculty in Donát Bánki College of Mechanical Engineering, where I graduated as an engineer in 1996. I began my research work as a third-year student under the supervision of Professor Imre Rudas, and I made it to the finals of the National Conference of Scientific Students' Associations with my essay titled "Entropy and similarity degrees of fuzzy sets".

I was recruited by the Office of National Security in 1997, where, after the training period, I commenced my work in the area of national security defence of law enforcement and key governmental facilities and institutions. My activity covered all dimensions of complex

information security; I collected, evaluated and analyzed the information and circumstances pertaining to the security status of the relevant organizations as well as made recommendations to provide information and take measures in order to eliminate various risks and threats.
Of the professional areas of complex information security, I was most interested in electronic information security, so I deepened my knowledge in this area, which allowed me to graduate as a defence system designer at Miklós Zrínyi National University of Defence in 2009.
Changing my professional area in 2010, I was involved in the key energetic and transport infrastructures of the Hungarian national economy and then went on working in the national security defence of key infocommunication infrastructures in 2012.

In relation with my professional activities, I have continuously participated in various scientific conferences, professional workshops organized by operators and the Hungarian partner organizations as well as professional consultations and further education courses arranged by foreign partner services.

In 2010, I was enrolled as a PhD student of cyber-terrorism, its methods and the potential defence alternatives at the Doctoral School of Military Technology of the National University of Public Service under the supervision of Col. Dr. László Kovács.

As the system security supervisor of the Ministry of Interior Affairs I have been involved in activities related to the security status of electronic systems managing classified data.

Budapest, 1st September, 2018

Zoltán István Papp