Denis Čaleta,
Gorazd Rolih

Pregledni znanstveni članek

KIBERNETSKA VARNOST V DRUŽBI IN DELOVANJE KRITIČNE INFRASTRUKTURE – ANALIZA STANJA NA OBRAMBNEM PODROČJU V REPUBLIKI SLOVENIJI

CYBER SECURITY IN THE OPERATION OF CRITICAL INFRASTRUCTURE – AN ANALYSIS OF THE SITUATION IN THE FIELD OF SLOVENIAN DEFENCE

Review paper

Povzetek Pojav asimetričnih oblik ogrožanja nacionalne in mednarodne varnosti izhaja iz popolnoma drugih predpostavk in dojemanj temeljnih konceptov zagotavljanja varnosti, ki je še nekaj časa po koncu hladne vojne temeljila na statičnem pristopu do obvladovanja konvencionalno opredeljivih vrst groženj. Spreminjajoče se družbene razmere in napetosti, ki jih je prinašal hiter tehnološki razvoj, so posamezna družbena okolja našle popolnoma nepripravljena na spopadanje z novo globalno varnostno situacijo. Zaradi navedenega bo treba kibernetskim grožnjam nameniti posebno pozornost. Učinkovito obvladovanje teh groženj je pomemben pogoj za nemoteno delovanje informacijsko-komunikacijskih sistemov, ki delujejo v okviru kritične infrastrukture. V Republiki Sloveniji bo treba ukrepe zoperstavljanja kibernetskim grožnjam načrtovati in izvajati v okviru sistemskega pristopa, saj si je zaradi omejenosti finančnih, kadrovskih in tehnoloških potencialov nemogoče zamisliti drugačno pot. Pri tem pa mora imeti obrambno področje, vključno s Slovensko vojsko, pomembno vlogo.

Ključne besede ***Kibernetske grožnje, globalna varnost, obrambni sistem, CERT[1], kritična infrastruktura.***

Abstract The emergence of asymmetric forms of threats to national and international security arise from completely different assumptions and perceptions related to the provision of security which, until recently, have been based on a static approach towards the management of conventional threats. As a result, changing social conditions and tensions (brought about by rapid technological development) have found individual social environments and classes completely unprepared for confrontation with this new, global, security situation. As the effective management of such threats is a significant condition for the smooth functioning of information and communication systems that are a part of critical infrastructure, cyber threats require special attention. In the Republic of Slovenia, it will be necessary to plan measures to counter cyber

[1] *Computer Emergency Response Team.*

threats and apply these on the basis of a systemic approach. Due to limited financial, personnel and technological potentials, it is impossible to think of a different course of action. In this context, the defence sector, including the Slovenian Armed Forces, must adopt a more active and significant role.

Key words ***Cyber threats, global security, defence system, CERT2, critical infrastructure***

Introduction

The globalisation of the world and, as a consequence, the globalisation of security, confronts modern society with demanding dilemmas. These dilemmas are, on the one hand, related to the question of how to continue to found one's development on the fundamental postulates of the free movement of goods, services and people and, on the other hand, of how to manage threats at an acceptable level of risk. The emergence of asymmetric forms of threats to national and international security arise from completely different assumptions and perceptions of the basic concepts related to the provision of security which, until recently, have been based on a static approach towards the management of conventional types of threats. The changing social conditions and tensions brought about by rapid technological development have found individual social environments and classes completely unprepared for confrontation with this new, global, security situation. The occurrence of non-state actors who have become involved in the interaction between traditional actors in international relations, has pushed to the surface new forms of security threats which are asymmetric in their form and can not be effectively countered through traditional systems and means. As a result of dynamic changes and unprecedented technological development, this dimension has become even more complex. The fact that modern society nowadays depends entirely on technology makes this society even more vulnerable from a security point of view, and individual threats and risks to the smooth operation of this critical infrastructure even more unmanageable[3]. Certain segments of this infrastructure are so important to the operation of society, that their failure or a limited operation could cause severe damage or problems to this society. This infrastructure is referred to as critical infrastructure. The authors of this article define critical infrastructure at the national and the international level, certainly depending on the effects caused by its failure or destruction.[4] Hence, according to the authors, two sectors should be particularly emphasised, namely the electricity supply and

[2] *Computer Emergency Response Team.*

[3] *62 percent of US critical infrastructure is directly linked with Internet or IP- networks (Secure Computing, 2008).*

[4] *"Slovenia's critical infrastructure of national importance encompasses those capabilities and services that are crucial for the state, and the failure and destruction of which would have a significant impact on national security, economy, key functions of society, health, security and protection as well as societal welfare." (Decision of the RS Government, No. 80000-2//2010/3, dated of 19 April 2010). In the EU context, definitions are as follows: "critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" and "European critical infrastructure" or "ECI" means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure (EU Council Directive, No. 114/2008, 8 December 2008).*

information and communication technology that have an interdependent impact on the operation of other sectors of critical infrastructure. Because of the above-mentioned arguments, this article focuses attention on cyber threats. Their effective management provides an important condition for the smooth functioning of information and communication systems that are part of critical infrastructure.

1 LITERATURE AND THEORETICAL STARTING POINTS RELATED TO THE SUBJECT MATTER

It can be established that - as a result of economic, sociological and cultural impacts - information and communication technology has become an indispensable part of the contemporary information society. As a matter of fact, it is impossible to imagine a society without an adequately functioning information and communication technology. In order to get a better understanding of this issue, it is necessary to provide a concrete definition of this technology. According to the European Union, this area includes the internet, the provision of stationary and mobile telecommunications, radio and satellite communications and transmitters. (Svete, 2010)

Possible threats to critical infrastructure in the area of information and communication technology may include natural threats and threats caused by man. These threats may also be divided further into intentional and unintentional threats. This article is limited to intentional threats, where terrorism plays a significant role. Especially since the terrorist attacks of September 11th, 2001, security experts strongly believe that information systems will be one of the next targets of terrorist attacks (cyber terrorism) (Weimann, 2006). The increased complexity of information systems poses a security challenge to developers and users. The analysis of the current development of cyber threats has shown that cyber terrorism does not represent a major threat. The EU Counter-Terrorism Coordinator argues that the threat comes mainly from various criminal networks and individuals who support and sponsor certain countries (De Kerchove, 2010).

Lukman and Bernik (2010, p. 5) have established that it is difficult to create a detailed classification of cyber threats, as new forms of attacks are constantly emerging and cannot be easily classified into known subgroups. Chakrabarti and Manimaran designed a taxonomy of the attacks on the internet infrastructure in response to previous classifications which were chiefly aimed at the protection and security of information. They divided attacks into four basic categories: DNS *"hacking*", routing table "*poisoning*", packet *"mistreating*" and "*denial-of-service*" attacks (Chakrabarti, Manimaran, 2003). To ensure confidentiality and the integrity of electronic communications, a number of cryptographic algorithms have been developed. However, these contain some security loopholes that may be exploited by system administrators as well as hackers in order to extract sensitive information from the encrypted network traffic (Kjaerland, 2005). The development of telecommunications infrastructure is directed towards merging the traditional telephone system and information technology into a unified platform. The accelerating expansion of wireless communication systems increases the possibilities of abuse. In this event,

the traditional defence approach to risks connected with cyber space, the virtual world and terrorism is given a more complex dimension. Collin defines the virtual world as "/.../ a place in which computer programs function and data moves" (Politt, 1997). Planning the information security of these systems requires a comprehensive approach and an exact implementation of all procedures. For the easy identification of hacking activities, software for their detection and alarming has been developed. Despite a high technological level however, software only becomes truly effective in conjunction with analysis. In this context, we may rediscover the significance of human potential and its role in the entire system of detecting the threats that have been discussed. Tun and Aung analysed the work of analysts and proposed a mechanism for intrusion visualisation (Tun in Aung, 2008). Intrusion alarm systems have also been studied by Kumar, who suggests a model for the automatic classification of the detected intrusion (Kumar, 1994). Despite the many classifications proposed for cyber attacks, all attacks on the systems of critical infrastructure can be divided into three main groups: intrusion into systems, disablement of service as well as attacks through malware (Lukman, Bernik, 2010).

Terrorism on the internet manifests itself in various ways, namely as a means for transmitting messages or as a tool for attacking individual targets. The World Wide Web has become a platform for international terrorism to spread its ideology, recruit and mobilise new members, collect funds and material support, disseminate messages of hatred and violence, search for information, conduct psychological warfare, plan and coordinate activities as well as to cross-communicate. Individuals also try to attack[5] computer networks, especially those connected to the world web. (Weimann, 2006)

2 METHODS

The analysis of the mechanisms for countering cyber threats conducted in this paper is based on the assumption that such complex threats at the national and international level can only be efficiently countered with adequately concerted and planned measures. The analysis provides a platform that allows an objective evaluation of the measures which are performed in the Republic of Slovenia with the aim of reducing and preventing cyber threats. In relation to this, the conclusion offers certain suggestions regarding the necessity of combining sources and mechanisms for prevention. This approach plays a particularly important role in small countries with limited human, financial, organisational and other resources.

The research question which occurs when studying the response mechanisms for cyber threats is, above all, whether the mechanisms and means established in the Republic of Slovenia allow for an adequate response to such a complex threat.

[5] *Numerous states are aware of the seriousness of the threats from the Internet and are establishing centres for the protection against cyber attacks (Malaysia has established the first International Multilateral Partnership Against Cyber Terrorism (IMPACT)) (Ko, 2008). NATO has established the Cyber Defence Centre of Excellence in Estonia (www.nato.int).*

In analyzing this research question, we will employ various indicators which show the support of political structures to the role of actors in the national security system. These indicators are, in general, limited to the following: (1) number of adopted statutory provisions, (2) number of prepared statutory provisions, (3) transparency of statutory provisions (number of submitted requests for the division of responsibility), (4) number of submitted initiatives for the change or supplementation of legal documents, (5) amount of budgetary funds, (6) statements of leading state politicians expressing their support, (7) presence and frequency of software and concept orientation and (8) practical implementation of the adopted legal solutions.

The authors of this paper attempt to draw conclusions based on current knowledge and lessons learned, and - above all - through various methodological approaches. In preparing this article, we mainly applied methods, such as qualitative analysis, historical qualitative analysis, description and content analysis.

The major limitations of the article are: (1) broad concept of the topic, opening a number of questions which, despite the implementation of the above-mentioned concepts, cannot be fully answered; (2) that conditions associated with cyber threats are constantly changing (Globalisation processes repeatedly open new possibilities for the emergence of various forms of threats and face us with the fact that something that has been established in this article today could be obsolete tomorrow.); (3) data on the organisation of countering cyber threats is classified in most counties and, hence, inaccessible to research work. Furthermore, it should be understood that the Republic of Slovenia is difficult to compare with other countries in terms of its resources.

3 SITUATION ANALYSIS

In order to assess the systematic approach to preventing cyber threats in the Republic of Slovenia and the situation of the defence system, a thorough analysis of the relevant legal documents and doctrines needs to be carried out. Given the findings that information and communication technology are nowadays associated with almost any field, the analysis of the legal basis will also be focused on the area of critical infrastructure protection, namely in the area where it is directly linked to cyber security. The analysis results are limited to the situation in Slovenia in comparison with the international environment, which the authors describe with reference to EU and NATO measures. This is followed by an overview of some of the most important documents related to cyber threats and protection against such threats, as defined by the EU and NATO. In the continuation we will analyse documents that have been adopted at the supranational level.

3.1 European Union

When addressing cyber threats, the protection of critical infrastructure, respectively critical information infrastructure (as its integral and extremely vulnerable element)

is of crucial importance. In December 2004, the EU Council adopted the European Programme for Critical Infrastructure Protection (EPCIP). Later, seminars were held which were attended by all member states and industrial associations as well as information security experts. The European Commission then prepared the Green Paper on a European Programme for Critical Infrastructure Protection. Defined were eleven sectors of critical infrastructure: energy, information and communication technologies, water supply, food, health care, finance, public & legal order and safety, civil administration, transport, chemical and nuclear industries, and space and research. These sectors were later limited in the European Council directive on critical infrastructure no. 114/2008 to only two sectors, namely transport and energy. The 2005 Green Paper on EPCIP provides the EU Commission's view on the way of organising European critical infrastructure (ECI) protection. This document defines general EPCIP objectives as the provision of adequate level protection measures associated with critical infrastructure, vulnerability reduction and the establishment of recovery mechanisms in the EU. Emphasis was placed on three areas: general threats, terrorism and likely targets. In a communication note issued after the Green Paper, the Commission called for an approach that fully took into account all forms of specific threats. The document also defines an approach which is directed to individual sectors. Given that the sectors comprise individual lessons learned, expert knowledge and requirements associated with critical infrastructure protection, each sector will form its individual EPCIP, which will be implemented based on agreement. The path leading to adopting the directive was difficult in the EU context.[6] The directive, however, does represent the beginning of the gradual identification and definition of European critical infrastructure as well as the implementation of the needs for improving its protection. Instead of the originally planned eleven sectors, the directive is now - based on a compromise solution - limited to energy and transport only. In the future, its effect and requirement to include other sectors will be evaluated. In this context, priority should be given to the information and communication technologies sector (Žel, 2011). The Republic of Slovenia, as a member state, must transpose the EU Council Directive No. 114/2008 of 8th December 2008 on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection (hereinafter the 'directive'), in its acquis[7]. The directive lays down a procedure for the identification and designation of European critical infrastructure as well as a joint approach for assessing the need to improve the protection of such infrastructure, in order to assure the protection of people. It comprises the energy and transport sector and can also be used for other sectors where the directive will be implemented.

---

[6] *At an informal meeting in Luxemburg in 2008, the Ministers of the Interior supported the idea that, instead of the directive, only a document of the EU Council Presidency should be drawn up that will include only a minimum common denominator related to this area. However, in May 2008, the decision was taken to adopt the directive, which was still objected to by Sweden. Due to many different opinions and approaches as well as the member states' different views regarding this matter, a curtailed directive was issued in 2008, which marks the beginning of ECI.*

[7] *Article 12 of the direcitive provides that member states shall implement the directive or adopt regulations, required for its implementation. The directive also sets a time frame, according to which it was necessary to submit the texts of the regulations of the member states and their correlation with the directive to the EU Commission by 12th January 2011.*

Similar activities are carried out in the area of critical infrastructure protection in the Republic of Slovenia. We began to study the problem of this type of protection after 2006, when a special inter-sectoral group for coordinating critical infrastructure protection (hereinafter inter-sectoral coordination group) was established. This group developed a special programme which included activities to enforce the Directive. The programme also included the definition of critical infrastructure of national importance, which is one of the few coordinated solutions related to this area. The inter-sectoral coordination group prepared a draft regulation which ensures the implementation of directives, but also regulates the protection of critical of national importance. Protection should be regulated in particular based on related provisions.

The original purpose of the inter-sectoral coordination group was to develop a proposed regulation (act or directive), summarizing the contents of the EU Council Directive 2008/114/ES as a whole and, at the same time, define the basis for arranging national critical infrastructure in related provisions, and to propose it to the RS Government for adoption. A special sub-group for developing a normative legal document regarding the implementation of the Directive 2008/114/ES was established. The group included representatives of the ministries of economy, transport, internal affairs, higher education, research and technology, defence, as well as representatives of the SAF General Staff and the RS Administration for Civil Protection and Disaster Relief. The group faced similar problems as the EU. Its only achievement was the harmonisation of the critical infrastructure definition, whereas all the remaining issues, including the proper definition of public and private partnership, have remained unresolved and controversial.

The Ministry of Defence[8], which is responsible for implementing the Directive 008/114/ES, has decided, given the fact that its introduction into Slovenian legislation expired as early as 12th January 2011, to develop only the Directive on European Critical Infrastructure. This decision was also impacted by a formal notice of the European Commission that stated that the national regulations related to the transposing of the Directive 2008/114/ES of 17 March 2011 had not been validated. Later, a relevant regulation was adopted and hence introduced into Slovenia's internal legal order.[9] The coordination of activities, as well as the legal bases and regulation of governing national critical infrastructure protection will be ensured separately. The problem lies mainly in determining adequate, reasonable and suitable measures of criticality, which are paramount for the development of regulations on critical infrastructure protection.

---

[8] *The fact that the Slovenian MoD is in charge of a coordination group for critical infrastructure protection is another special feature of Slovenia. In other countries, this task was assigned to ministries responsible for internal affairs or to special government service. This can be explained by the fact that the MoD has been previously in charge of civil defence, which now also covers critical infrastructure. Another fact is that after the changed social conditions, some sectors seek a new position in the system of providing individual areas of national security.*

[9] *RS Official Gazette, No. 35/01, dated 13 May 2011.*

3.2 NATO

The last strategic concept (2010, p. 4), adopted in November 2010 at the Lisbon Summit, identified cyber threats as very serious, more frequent, better organised and more devastating whatever the target of the attack (e.g. government administrations, businesses, economies and other organisations). NATO considers critical infrastructure a potential hazard as, in the event of its failure, it could threaten national and North-Atlantic interests, prosperity, security and stability. According to NATO, possible sources of such attacks can be intelligence services, organised criminals, terrorist and extremist groups. NATO will hence include technology-related trends into its planning processes and future operations.

In accordance with the strategic concept (2010, p. 5), NATO will develop and employ its capabilities to deter and defend against the following threats (list related only to cyber threats):
- Systems to prevent detect and defend against and recover from cyber attacks, including planning processes for enhancing and coordinating national capabilities as well as the centralized protection, awareness, warning and response of all member states.
- Development of the capacity to protect energy sources, including critical infrastructure.

NATO's legitimate and legal rights to protect its member states are also ensconced in Article 5 of the North Atlantic Treaty[10]. Still, there are certain issues with this context, namely that this document was drafted and adopted at a time when IT-related threats were not known and that the document defines only armed attack. The use of this article in response to a cyber attack would be legally questionable; even in the case the motive was established and the attacker was identified. In addition, there is also the question of how to adequately respond to an attack. Cyber attacks usually involve thefts, falsifications or deletion of data, yet direct physical damage and human casualties do not occur. Is the use of forces thus justified?

The use of Article 5 of the North Atlantic Treaty has been intensively supported by US foreign policy. Accordingly, attacks will no longer be conducted from the air or through conventional weaponry, but via optical cables and it will be necessary to strongly respond to cyber attacks, particularly if they target critical infrastructure (Amies, 2010).

Bruce Schneier (2010), on the contrary, believes that cyber crime has become an everyday practice and that the Estonian events[11], for example, were nothing more

[10] *North Atlantic Treaty Article 5 consists mainly of the idea that an armed attack against one of the members is percieved as an attack on all.*

[11] *In April 2007, Estonia was hit by "Denial of Service"-attacks (DDoS - attacks, in which a target site is bombarded with so many bogus requests for information that it crashes) by alledged Russian hackers, which disenabled vital servers and, temporarily, almost the complete functioning of the Estonian banking system and government (Layden, 2007).*

than an act of ethnically upset Russian hackers protesting against anti-Russian policy in Estonia. He condemns hacker activities and perceives them as a serious threat. However, he notes that in the vast majority of cases, it is the result of activities performed by children and fanatics. He argues that whilst the building of offensive and defensive cyber war capabilities is absolutely legitimate, that it is necessary to avoid abuse. In this context, he highlights key problems, such as supported motives and the identification of attacker. Yet it is very difficult or even impossible to identify it. Schneier notes that cyber war is equally likely as conventional and expects the simultaneous use of both forms in the event of war. He strongly supports the opinion that we need only a peace-time information security, which is based on the synergy effect of various private and public organisations.

NATO's first step towards the setting up of joint capabilities in the fight against cyber threats has been achieved by the establishment of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia. The centre, which is not part of NATO's command structure, was accredited on 28th October 2008 in Tallinn (Estonia) and is financed by the founding countries and sponsors. The centre does not deal with cyber incidents, which is a matter for the NCIRC (NATO Computer Incident Response Capability). Tasks of the CCDCOE are to:

- Enhance and broaden awareness of threats to information security among NATO member states and partner countries, namely through education, research and development as well as the provision of information and support in the process of *lessons learned*;
- Support NATO in the search for best practices, patterns, concepts and strategies and the legal basis for the conduct of information warfare.
- Provide, at the tactical level, technical solutions, security systems in tactical environments, the identification of cyber threats and attacks as well as recovery after intrusion, system control and interoperability development.
- Protect critical systems.
- Develop methodologies for risk and security assessment.
- Develop modelling and simulation technologies related to cyber threats (NATO Cooperative Cyber Defence Centre of Excellence, 2011).

3.3 National level

Below, we will introduce and analyse strategic documents and bodies at the national level, which include provisions that are related to and were established for the identification, prevention of and response to cyber threats.

National Security Strategy

The governments of some countries[12] have, after numerous cyber incidents, become aware of the increase and seriousness of such events. In the Resolution on National Security Strategy, which entered into force in March 2010, the Republic of Slovenia

[12] *In British National Security Strategy (NSS), which was issued in October 2010, cyber attacks and cyber were rated second highest in the first class of risks (NSS, 2010, p. 27).*

listed the following incidents as sources of risk to national security: terrorism, illicit activities in the area of conventional weapons, weapons of mass destruction and nuclear technology, organised crime, illegal migrations and, of course, cyber threats. The document states:

"On account of the diversification of information and communication systems, boundlessness of cyberspace and problems related to its control, the Republic of Slovenia may expect an expansion in various forms of cyber crime, particularly cyber intrusions and attacks on state and non-state entities, which will be impossible to limit in space and time (ReSNV-1, 2010, p. 7)."

According to the Resolution, the likelihood of asymmetrical threats will increase and, in addition to land, sea, and air, the future theatre of war will also include the cyber environment. In response to cyber threats and the misuse of information technologies and systems, the document states:

"With regard to cyber security, the Republic of Slovenia will create a national agenda for responding to cyber treats and the misuse of information technologies, and adopt necessary measures to ensure effective cyber defence which will, to the maximum extent possible, include the public and private sector. One of the priority tasks in ensuring cyber security will be the establishment of a national coordination body (ReSNV-1, 2010, p. 16)."

Nevertheless, these strategic documents do not include answers to the question of how to solve the key issue of public and private partnership, which is crucial for the effective prevention of and response to cyber threats to information and communication critical infrastructure.

A clear distinction between the public and private sector with regard to the area of critical infrastructure protection is slowly but persistently disappearing, up to the point where there is no overall responsibility for a particular segment but a shared responsibility. It is an undeniable fact that the majority of critical infrastructure is in private ownership. This means that the state itself is no longer able to ensure comprehensive security of this critical infrastructure and depends largely on the exchange of information and joint measures with participating partners. A well-defined public-private partnership represents a factor which is essential for ensuring a comprehensive and successful policy for critical infrastructure protection. In that regard, it is necessary to have a comprehensive vision, together with an appropriate strategy and strong political commitment, to reach the desired state. In order to reach the desired level of awareness, such a vision has to be communicated to all owners of critical infrastructure. The vision, strategy and appropriate level of awareness can be described as the fundamental basis for an effective policy for critical infrastructure protection. (Čaleta, 2011)

CERT (Computer Emergency Response Team)[13]

Currently, CERTs are an essential instrument for protecting critical infrastructure. All countries that are connected to the internet must have capabilities to effectively respond to computer-related incidents. These capabilities are a primary source for the protection of a state and its population (Porenta, 2011). The SI-CERT (Slovenian Computer Emergency Response Team) is the Slovenian national computer emergency response team, which is tasked with responding to internet-related incidents, coordinating work and informing on and solving security problems in Slovenian computer networks. SI-CERT serves as a point of contact, providing mediatory and advisory services. It operates as part of the Arnes-network (Academic and Research Network of Slovenia), yet, as the name suggests, it only accepts notifications of security incidents in Slovenian computer networks. Arnes and the Ministry of Public Administration signed, based on the decision of the RS Government of 31st May 2009, an agreement on cooperation in the area of information security. The agreement sets out that Arnes SI-CERT will provide assistance in establishing a government centre. Meanwhile, it will coordinate all responses to security incidents for all public administration information systems. The governmental CERT centre will specialize in the public administration network and systems, while SI-CERT will continue to be a national point of contact (Božič, 2011). The Ministry of Defence (MoD) also organised a CERT, whose operation is defined in the Instructions for Implementing Measures during Security Events and Incidents in MoD CIS (No. 007-70/2008-1 dated of 6 March 2008). The instructions provide organisational and technical measures for ensuring services of the computer emergency response team during security events and incidents in MoD CIS.

It should be noted that the area affected by cyber security is extremely wide, a fact that is reflected in the extent of legal documents which indirectly or directly affect the subject matter. The Republic of Slovenia, therefore, has adopted regulations associated with this area, namely the Personal Data Protection Act, the Access to Public Information Act, the Electronic Commerce and Electronic Signature Act, the Electronic Communications Act, the Classified Information Act and the Decree on Administrative Operations and other documents.

4 SITUATION ANALYSIS OF THE DEFENCE AREA

Information Security Council

The Information Security Council operates under the Ministry of Defence. A significant portion of its tasks currently focuses on increasing NATO efforts with the purpose of developing a joint cyber defence concept, where all member states, including Slovenia, assume an equal role. The Alliance's objectives, arising from the

[13] *The first CERT was established in the USA in 1988 and founded by ARPA (Advanced Research Projects Agency), in response to the first major internet incident – the speading of the first worm, later referred to as the Internet Worm. With the expansion of the internet, similar organisations began to appear elsewhere in the world (CERT-SI, 2011).*

Lisbon Declaration, are to upgrade the communication and information systems and to achieve full capability in cyber defence by 2012. Each member state shall establish active CERT capability, make proper efforts to improve the security culture, launch centrally managed networks and systems, as well as define and establish a system for critical infrastructure protection. According to the majority of member states, critical infrastructure (which is a frequent target of internet attacks) constitutes a key element in forming the joint cyber defence concept. In view of enhancing the rational use of resources, some members have stressed the importance of the cooperation between the EU and NATO, as well as between the national CERTs (Computer Emergency Response Teams) and the NCIRC (NATO Computer Incident Response Capability). In formulating the cyber defence concept, NATO member states are harmonizing the three areas included in the responsibility of a harmonised NATO cyber defence:

– All NATO networks, networks that support the Alliance's operation and networks for supporting the operation of commands and agencies.
– All national communication networks which are included in NATO operations.
– All civil networks of member states, which are crucial for the operation of national critical infrastructure.

In discussing the concept, member states have reached an agreement regarding the first two areas, yet not regarding the third area. The reason for this is that some member states are reluctant to include the third area into the NATO concept.

The Information Security Council appointed a working group at the MoD in 2011 for harmonising viewpoints on cyber defence before national treatment. The group is currently, before the viewpoints are discussed at the national level, preparing a proposal of MoD activities for the drafting and implemention of the cyber defence concept. This position is focused on national and international efforts, the upgrading of communication and information systems and the establishment of an effective cyber defence capability. In doing so, the MoD supports the activities of NATO, the EU and individual member states for creating collective and national cyber defence capabilities. The inter-sectoral cooperation and the cooperation within the Alliance are of essential importance in formulating the concept and national strategy of cyber defence. It was agreed to appropriately apply solutions of good practices which have already been implemented in EU and NATO member states and to adapt them to Slovenia's national requirements. In this context, critical infrastructure protection is a decisive factor, although it has not as yet been defined as such. The MoD will hence expand its cooperation with the NCIRC, which provides capabilities for responding to computer-related incidents.

4.1. International comparison of the defence area

Mechanisms for international and national legislation have often proved ineffective in combating global cyber threats. The reasons might be as follows:

– Lack of a comprehensive and centralised control over the internet, as well as communication and information systems.
– Information threats are not dealt equally by all states.

– Exceptionally demanding or even impossible identification of attackers.
– Difficulty or impossibility to identify an attacker's motive.
– New technologies are always one step ahead of the law.
– National legislation of individual countries outside their borders is not always effective.

For the time being, a common agreement has not been achieved on what cyber threat actually is, and how to identify, prove and sanction it. In most cases, the international community is aware of the seriousness of the problem, yet there is no universal or common solution to the problem (Bosworth, Kabay, 2002, p. 7). The article continues with an overview of capabilities for countering cyber threats of selected countries. This overview will facilitate the understanding of the situation and the position of this issue in the Slovenian defence area.

The US military earmarks probably most resources, both financial and human, to developing capabilities in the area of cyber warfare. In the spring of 2010, US Defence Secretary Robert Gates announced the launching of the U.S. Cyber Command - CYBERCOM. Half a year later, the unit became fully operational and is commanded by Three-Star General, Rhett A. Hernandez, a clear demonstration of the importance of this command. It will eventually consist of as many as 21,000 members, recruited from the ranks of the best computer experts and hackers. As it was emphasised, only the best members will be prepared for possible operations. In the USA, a great deal of. Attention will also be dedicated to its forensic capabilities as legal aspects are considered of particular importance. Attackers will most likely use a variety of ways to obliterate their tracks, due to which they need to be traced down and identified. Furthermore, it has also been stressed that cyber defence cannot function alone and that it is also necessary to building offensive methods is a key element of effective defence (Miles, 2011).

The German Bundeswehr also established a special unit of so called hackers in uniform. Currently, the unit is referred to as the Department for Information and Computer Networks Operations (Abteilung Informations- und Computernetzwerkoperationen). Their task is to conduct training in defence and counter-attacks against cyber threats. The Federal Government has, at the same time, also changed the Federal Office for Information Technology Security (Bundesamtes für Sicherheit in der Informationstechnik – BSI) into a cyber defence agency, thus making more funds and human resources available to the agency (Mann, 2009).

In its national security concept of 2000, Russia identified cyber threats as threats to its national security due to an increased development of cyber warfare concepts in other countries. This document states that a US cyber attack will be understood as a military threat and that Russia will strongly respond to it, perhaps even by using nuclear weapons. The prominent Russian University in Tomsk is known for educating acknowledged cyber warfare experts. Yet, unfortunately, some of them also offer their knowledge to hacker organisations. Based in Russia, is the notorious

Storm Botnet Network, which is a network consisting of several computers of unsuspecting internet users around the world. The malicious code, by which these computers were affected, is not harmful by itself, yet it is prepared for the commands of those who are managing this network (CDCOE, 2010).

China is also successfully following global trends and it is assumed, as with other world powers, that the country is developing its information technology capabilities. The process of modernizing and computerizing China's armed forces includes also the training of soldiers for cyber warfare, which is taking place in modern computer labs. This trend is also supported by the university through studying cyber defence and attacks, hacker methods and malicious codes. China pays special attention to *cyber reconnaissance* or interceptions of internet traffic. For example, China successfully managed to exploit the vulnerability of the Boarder Gateway Protocol (BGP) and diverted 10 percent of global internet traffic to its routers. Prior to that, the Chinese stated that they had managed to develop the most powerful computer in the world. Theoretically, it is possible that such a machine could analyse internet traffic, yet a connection between these two events could not be proven (Fritz, 2008). The Chinese doctrine dedicates particular attention to asymmetric operations. China is a vast country with a large population that is gradually turning into a global, economic power. As a consequence, it is taking advantage of the development of its capabilities for offensive cyber operations and reconnaissance and collecting various intelligence to strengthen its economic and military power. Many traces of cyber attacks, including the infamous attack on Google servers lead to China and this is not only good evidence of how technologically well-developed the country is but how successfully it has been following global trends (Fritz, 2008).

However, Chinese authorities have only admitted to one unit called the *Blue Army* which is allegedly composed of just 30 acknowledged military and civilian computer experts that have been exclusively trained for defensive operations. This secrecy confirms the fear of many governments in the world that computer systems can be - at any time – the target of Chinese attacks (McConor, 2011).

4.2. Defence System of the Republic of Slovenia

In its strategic documents (ReSNV-1), the Republic of Slovenia identified cyber threats as risks to national security and has committed itself to prepare a national strategy for responding to such threats. The measures for effective cyber defence will, as far as possible, include the public and private sector. One of the priorities in providing cyber security will be the establishment of a national coordination body for cyber security. In its Resolution on General Long-Term Development and Equipping Programme of the Slovenian Armed Forces up to 2025 (adopted in November 2010), Slovenia recognises that the future theatre will, in addition to land, sea, and air, include both cyber space and outer space. The SAF will pay special attention to the development (among other capabilities) of capabilities for computer and communication systems for protection against cyber attacks. It will also develop cyber warfare capabilities, among others, as multipliers of combat

power. Also, it will introduce a safe and flexible communication and information network infrastructure, complying with the requirements of NATO capabilities of network operation. Introduced will be measures and capabilities for information security, dedicated for the prevention of uncontrolled access and inclusion into the network (adapted from ReSDPRO, 2010).

In this document, the Slovenian Armed Forces have committed themselves (ReSDPRO 2025) to pay, in the future, particular attention to the development of computer and communication systems for the protection against cyber attacks as well as to develop cyber warfare capabilities as multipliers of combat power. The draft of the Mid-term Defence Programme (SOPR, 2011–2016), which was submitted to the Government for approval, states that measures of cyber defence in the SAF will be carried out in accordance with the Alliance and the national strategy (SOPR 2011, p. 9).

According to EU documents and the EU Programme for Critical Infrastructure Protection, a range of legal documents were adopted at the national and MoD level. Although the MoD established its own national CERT, it has as yet to come to life. The working group, including members of the MoD, SAF and other ministries, participates in the establishment of a government CERT in cooperation with the SI-CERT which currently serves as a national point of contact, providing mediatory and advisory services.

After the Estonian attacks, NATO as well began to seriously respond to cyber threats. It established the Centre of Excellence in Estonia, in which it develops capabilities for providing support to the joint efforts in the combat against cyber threats. Currently, the Alliance is intensively developing a joint cyber defence concept. In discussing the document, the member states have reached an agreement in principle on the first two areas, while the third one has not been agreed on, as some countries were reluctant to include theirs into the competence of NATO's coordinated cyber defence. Slovenia has established a working group for the preparation of the national cyber defence strategy, taking examples of good practice as a starting point. The Slovenian Armed Forces participate in the development of the national strategy and cyber defence concept with only two representatives being present in the working group. For the time being, it does not dispose of resources for developing its own capabilities.

As a result of new features, such as the inclusion of national critical infrastructure into the NATO concept and the preparation of the national cyber defence strategy and concept, it was necessary to establish a national coordination body for cyber security as soon as possible. Besides the fact that Slovenia needed to make its contribution to the Alliance, it also had to protect its national interests, sovereignty and the autonomy of its critical infrastructure. Slovenia committed itself to this in its Resolution on the National Security Strategy. In our opinion, as the coordination body concerns political and expert decisions, it should be composed of a group of experts from the public and private sectors and the universities. It should also be given the remit to coordinate national, Alliance and EU activities and the responsibility and resources

to implement them in accordance with the principles of the good practices developed from the Estonian example and in line with other major countries such as Germany (Bundesamtes für Sicherheit in der Informationstechnik – BSI). As critical infrastructure is under the responsibility of various ministries, authorisations received by relevant bodies are a decisive factor and the National Coordination Body for Cyber Security would therefore be better placed within the organisational structure of the National Security Council, whose main activities are connected with the provision of national security.

The Slovenian Armed Forces have to more actively participate in the processes for providing cyber security through representatives in the national cooperation body and the development of its capabilities and knowledge. In this context, it has to consider the current issues regarding its staffing conditions. As the Slovenian Armed Forces committed itself to introducing its cyber defence capabilities into the ReSDPRO 2025, the development of these capabilities is necessary. This is due to classified information which has to be protected, the specific nature of the work and the vast number of communication and information systems of the Slovenian Armed Forces. Furthermore, in order to ensure a smooth command and control process (PINK) and follow the example of most developed militaries, the armed forces needs to ensure (as far as possible) sovereignty over these communication and information systems. It should, therefore, test and compound its knowledge and skills through greater participation in the increasing number of international cyber exercises taking place across NATO. In this context, the annual NATO Cyber Defence Exercise - which will be organised by the European Network and Information Security Agency, ENISA - should be mentioned. The seriousness with which the Slovenian Armed Forces considers cyber threats should not be underestimated, an indication of which can be seen from its inclusion of cyber incidents to the scenario of its Spring 2011 Exercise.

Conclusion

It is no longer a question of *if* a Cyber attack occurs, but *when*. Today, we are interested in how it will happen, how prepared we are and how devastating it will be. This assumption is based on numerous examples from the recent past and the fact that such occurrences are becoming more frequent, better organised and increasingly devastating. The realisation of cyber threats could have serious consequences if we are unprepared. For example, the operation of key systems for the normal operation of society could be paralyzed. In the worst case scenario, cyber attacks could result in devastating the economy and causing a massive loss of life.

The means through which potential attackers could implement their threats are well-know to us, and even the techniques and methods they use. However, a sufficiently reliable defence and protection system does still not exist. Currently, states individually address the problem by organising CERT centres to cope with the challenges of the cyber attacks. Some states, such as the USA, Great Britain, Germany and others, have placed an emphasis on cyber threats and incorporated counter measures into their national security strategies. In addition, they have launched

centres and agencies that coordinate activities at the national level. Above all, the militaries of these countries are intensively building up capabilities thorough which they can more effectively combat cyber challenges. These states are also strongly aware of the importance of integrating various national institutions and the importance of the interoperability and cooperation between states, in particular at the EU and NATO level. In comparison to large countries, the Slovenian Armed Forces does not possess capabilities for countering cyber threats due to its small size. However, they do attempt to follow global standards by educating experts at home and abroad and by liaising with civilian institutions and universities in the area of development and education. The legal basis required for the development of capabilities to combat cyber threats is also defined in doctrines at the national level (ReSNV-1) and the MoD level (ReSDPRO, 2025). Furthermore, activities are being carried out to develop the cyber defence concept and a national strategy, in which critical infrastructure protection plays a key role. Unfortunately, it is still not fully defined, functional, nor harmonised at the inter-sectoral level. This paper has established that its development should be based on the concept of good practices outlined above and that the activities of NATO, the EU and individual member states are paramount. In addition, cooperation not only with the public and private sectors but with academic and educational institutions is integral to its success.

At present, the Slovenian Armed Forces have neither the personnel nor resources to achieve this level of security. Even a concept for establishing cyber warfare capabilities (to which they had legally committed themselves) has failed to materialise. In fact, the majority of cyber activities are currently being carried out by the administrative part of the MoD with the actual SAF playing but a minor role.

Warfare in cyber space is a fact which, from the national security point of view, is much more serious than it might seem. The Slovenian Armed Forces should hence be fully supported in considering cyber warfare as an integral part of their remit and sufficiently resourced to effectively counter the threat.

References

1. *Amies, F., 2010. NATO includes threat of cyber attack in new strategic concept document, http://www.dw-world.de/dw/article/0,,6072197,00.html (6. 6. 2011).*
2. *Bosworth, Seymour; Kabay, M. E., 2002. Computer Security Handbook. New York: John Wiley & sons, INC.*
3. *Božič, G., 2011. How strong is your cloud?. Zbornik mednarodne konference »Kaj nam prinaša računalništvo v oblaku?«, Armes, Kranjska gora, str.10–12.*
4. *Schneier, B., 2010. It Will Soon Be Too Late to Stop the Cyberwars, http://www.schneier.com/essay-334.html (12. 12. 2010).*
5. *Chakrabarti, A., in Manimaran, G., 2003. A Case for Tree Migration and Integrated Tree Maintenance in QoS Multicasting. Dostopno na http://www.arnetminer.org/dev.do?m=downloadpdf&url=http://arnetminer.org/pdf/PDFFiles2/--d---d-1253857098812/A Case for Tree Migration and Integrated Tree Maintenance in QoS Multicasting1253872172718.pdf (22. 4. 2011).*
6. *Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, http://www.ccdcoe.org/11.html (14. 12. 2010).*

7. *Čaleta, D., 2011. A comprehensive approach to the management of risks related to the protection of critical infrastructure: public-private partnership. Caleta, D., Shemella, P. (Ed.) Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection. Institute for Corporative Security Studies and Centre for Civil Military Relations, Ljubljana.*
8. *De Kerchove, G., 2010. Eu Counter terrorism strategy – Discussion paper. Counil of the European Union, number 158941/10 (rev. 1) z dne 29. 11. 2010.*
9. *Direktiva sveta (ES) o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite, št. 114/2008 z dne 8. decembra 2008.*
10. *Dunn, M., Wigert, I, A., 2006. International Critical Information Infrastructure Protection (CIIP) Handbook.*
11. *Frtiz, J., 2008. How China will use cyber warfare to leapfrog in military competitiveness. Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80, http://www.international-relations.com/CM8-1/Cyberwar.pdf (12. 5. 2011).*
12. *Kjaerland, M., 2005. A classification of computer security incidents based on reported attack data, Journal of Investigative Psychology and Offender Profiling, Volume 2, Issue 2, str. 105–120.*
13. *Ko., C., 2008. Network World Canada, 4. jul. 2008, Vol. 24, Issue 13.*
14. *Kumar, S., in Spafford, E., 1994. An application of Pattern Matching in Intrusion Detection, Tecnical Report. West Lafayette: Purdue University.*
15. *Leyden, J., 2007. Estonia has faced down Russian rioters, http://www.economist.com/node/9163598 (dne 30. 08. 2011).*
16. *Lukman, M., Bernik, I., 2009. Ogrožanja kritične infrastrukture iz kibernetskega prostora. 10. Slovenski dnevi Varstvoslovja, Zbornik prispevkov, FVV, Ljubljana, 4–5. junij 2011.*
17. *Mann, U., 2009. Spionage - und Hackerabwehr Bundeswehr baut geheime Cyberwar-Truppe, http://www.spiegel.de/netzwelt/tech/0,1518,606096,00.html (12. 6. 2011).*
18. *Miles, J., 2011. Army Cyber Command Focuses on Protecting Vital Networks. http://www.defense.gov/news/newsarticle.aspx?id=65031 (dne 30. 8. 2011).*
19. *McConor, J., 2011. China's Blue Army of 30 computer experts could deploy cyber warfare on foreign powers, http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826 (30. 8. 2011).*
20. *Politt, M., M., 1997. Cyberterrorism – Fact or Fancy? FBI Laboratory, Washington D. C., dostopno: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (9. 10. 2006).*
21. *Panagiotis, T. (Ed.), 2011. Inter X: Resilience of the Internet Interconnection Ecosystem Summary Report – April 2011 http://www.enisa.europa.eu/act/cert (30. 8. 2011).*
22. *Porenta, J., 2011. Cloud computing at Arnes. Zbornik mednarodne konference »Kaj nam prinaša računalništvo v oblaku?«, Armes, Kranjska Gora, str. 7–9.*
23. *Resolucija o splošnem dolgoročnem programu opremljanja in razvoja slovenske vojske do leta 2025 (ReSDPRO 2025), 23. 11. 2010, številka 200-03/10-29/15.*
24. *Resolucija o strategiji nacionalne varnosti Republike Slovenije, št. 200-01/10-5/22, Ljubljana 2010.*
25. *SI CERT, http://www.cert.si/varnostne-groznje.html (3. 11. 2010).*
26. *Srednjeročni obrambni program 2011–2016 (osnutek), Generalštab Slovenske vojske 2011.*
27. *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010. Konferenca NATA v Lizboni.*
28. *Svete, U., 2006. Nacionalnovarnostni vidiki ogrožanja informacijske infrastrukture. V: PREZELJ, Iztok (ur.). Ogrožanje nacionalne varnosti, Varstvoslovje, Letn. 8, št. 1. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede, 2006, str. 31–44, graf. prikazi.*

29. *Svete, U., 2007. Informacijske razsežnosti sodobnega terorizma-teoretična vprašanja in praktični vidiki. UJMA, št. 21/2007, str. 124–129.*
30. *Svete, U., 2010. Informacijska in komunikacijska kritična infrastruktura. V: PREZELJ, Iztok (ur.). Kritična infrastruktura v Sloveniji, Knjižna zbirka Varnostne študije. Ljubljana: Fakulteta za družbene vede, 2010, str. 43–63.*
31. *Tun, Z., Aung, H., M., 2008. Wormhole Attack Detection in Wireless Sensor Networks, Proceedings of world academy of science, engineering and technology, Volume 36, december 2008, http://www.waset.org/pwaset/v36/v36-94.pdf, (21. 2. 2011).*
32. *Uredba o evropski kritični infrastrukturi, Uradni list RS, št. 35/01 z dne 13. maja 2011.*
33. *Weimann, G., 2006. Terror on the Internet - The New Arena, The New Challenges. Washington D.C.: United States Institute of Peace Press.*
34. *Žel, R., 2011. Obrazložitev k predlogu za sprejem Uredbe o evropski kritični infrastrukturi. DOZ, MO RS, 10. 2. 2011.*