Sodobni vojaški izzivi

Contemporary Military Challenges

Znanstveno-strokovna publikacija Slovenske vojske

ISSN 2232-2825
November 2011 – 13/št. 3

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
GENERALŠTAB SLOVENSKE VOJSKE

Sodobni vojaški izzivi

Contemporary Military Challenges

Znanstveno-strokovna publikacija Slovenske vojske

ISSN 2232-2825
UDK 355.5(479.4)(055)

November 2011 – 13/št. 3

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
GENERALŠTAB SLOVENSKE VOJSKE

Izdajatelj Publisher	Generalštab Slovenske vojske General Staff of Slovenian Armed Forces
Glavni urednik Executive Editor	brigadir Branimir Furlan
Odgovorni urednik Managing Editor	dr. Liliana Brožič
Uredniški odbor Editorial Board	VVU XIII. razreda dr. Valerija Bernik VVU XIV. razreda dr. Denis Čaleta polkovnik dr. Tomaž Kladnik brigadir dr. Andrej Osterman dr. Rado Pišot dr. Jože Plut dr. Uroš Svete
Sekretarka Secretary	Iris Žnidarič
Uredniški svet Editorial Council	dr. Andrej Anžič dr. Anton Bebler dr. Sabine Collmer dr. Damir Črnčec generalmajor Ladislav Lipič dr. Thomas Mockaitis generalpodpolkovnik dr. Iztok Podbregar dr. Tibor SzvircsevTresh
Prevajanje Translation	Ana Hazler Christopher McKeating Nataša Simonovič Bakoš Mateja Švab Iris Žnidarič
Lektoriranje slov. besedila Proofreading	Milena Sevšek Potočnik
Oblikovanje Design & Graphic	Skupina Opus Design
Tisk Print	Tiskarna Collegium graphicum, d. o. o.
Naklada Edition	500 izvodov/copies
Revija je dostopna na spletni strani Publication web page	http://www.slovenskavojska.si/publikacije/sodobni-vojaski-izzivi/ http://www.slovenskavojska.si/en/publications/contemporary-military-challenges/
E-naslov urednice Managing Editor e-mail address	liliana.brozic@mors.si

Hibridne grožnje

»Vsi živimo pod istim nebom,
pa nimamo istega horizonta.«

Konrad Adenauer

Hybrid Threats

»We all live under the same sky,
but do not all have the same horizon.«

Konrad Adenauer

RECENZENTI/REFEREES

Dr. Denis Čaleta
Dr. Damir Črnčec
Dr. Tomaž Kladnik
Dr. Igor Kotnik
Dr. Matej Kovačič
Dr. Jure Medič
Dr. Anže Rode
Dr. Uroš Svete
Primož Šavc

VSEBINA
CONTENTS

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.0

Liliana Brožič

UVODNIK

Letošnja tretja številka Sodobnih vojaških izzivov je v celoti v angleškem jeziku, s čimer sledimo programu dela uredniškega odbora in standardom kakovostnih znanstveno-strokovnih publikacij, tako v Republiki Sloveniji kot v širšem mednarodnem prostoru.

Številko smo posvetili hibridnim grožnjam. Definicijo hibridnih groženj in njihov razvoj pojasnjuje **Jan Spišák** v svojem članku o hibridnih grožnjah in razvoju novega Natovega splošnega koncepta. V njem pojasni tudi razumevanje hibridnih groženj v zavezništvu in načine odzivanja nanje.

Med hibridne grožnje spadajo tudi tako imenovane kibernetske grožnje, ki so vedno bolj domišljene, organizirane in povzročajo vedno večjo škodo državam, podjetjem, infrastrukturi in logistiki, tako v varnostnem kot finančnem smislu.

Aktualnim težnjam kibernetskega prostora v obdobju WEB 2.0 sta se posvetila **Uroš Svete** in **Anja Kolak,** in sicer s poudarkom na primeru WikiLeaks, v katerem je posebej izražen razvoj druge generacije svetovnega spleta, torej generacije, ki jo neposredno oblikujejo uporabniki sami in lahko tako tudi ogrozijo nacionalno varnost posamezne države ali zavezništva.

O pomembnosti in organiziranosti kibernetske varnosti v povezavi s kritično infrastrukturo pišeta **Denis Čaleta** in **Gorazd Rolih.** Predstavljata urejenost področja v Evropski uniji, Natu in na nacionalni ravni ter opozarjata na nekatere pomanjkljivosti, ki bi jih bilo treba še urediti.

Informacijsko varnost in njen pomen za javno upravo predstavlja **Maja Bolle** na primeru primerjave odprto- in zaprtokodne programske opreme. Seznani nas z njuno zgodovino in načinom delovanja ter prednostmi in slabostmi pri izbiri ene

izmed njiju. Seveda pa izbira ene ali druge prinaša številne izzive, o katerih avtorica razpravlja.

Avtorji **Anže Rode, Kristian Beršnak** in **Bojan Langerholc** predstavljajo Enoto za specialno delovanje Slovenske vojske ter njeno vpetost v širši nacionalni in nadnacionalni varnostni kontekst, s poudarkom na morebitnem delovanju v kriznih razmerah in protiterorističnih aktivnostih.

Kritični pogled na sicer že splošno sprejeto teorijo Karla von Clausewitza sta pripravila **Zoltán Jobbágy** in **László Szegő**. Preverjala sta jo na najnovejših spoznanjih na primeru Iraka in Afganistana, bralcem pa predstavljata svoja razmišljanja.

Članki slovenskih avtorjev, ki so bili napisani v slovenskem jeziku in pozneje prevedeni v angleški jezik ter tako tudi natisnjeni, so slovenskim bralcem na voljo v elektronski obliki na spletnih straneh Sodobnih vojaških izzivov, v posebnem dodatku na koncu publikacije.
Tako poskušamo ob upoštevanju racionalne rabe virov in kakovostnih kazalcev, ki veljajo za periodične znanstveno-strokovne publikacije, doseči čim širši krog bralcev in morebitnih piscev.

Vse naše bralce prijazno vabimo k pisanju člankov!

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.00

Liliana Brožič

EDITORIAL

This year's third issue of Contemporary Military Challenges is entirely published in English, which is in line with the Editorial Board's work programme and standards for scientific and professional publications in the Republic of Slovenia as well as widely abroad.

The present issue is dedicated to hybrid threats. The definition of hybrid threats and its development is explained by **Jan Spišák** in his article on hybrid threats and the development of NATO's new Overarching Concept in which he explains the understanding of hybrid threats within the Alliance and the ways of responding to them.

Hybrid threats also include the so-called cyber threats, which are becoming increasingly well though out, organised and causing more and more damage to the states, companies, infrastructure and logistics in a security and financial sense.

Current cyber space trends in the WEB 2.0. age have been dealt with by **Uroš Svete** and **Anja Kolak** who put emphasis on the WikiLeaks case, highlighting the development of the second generation of World Wide Web, which can be directly modified by the users themselves, thereby threatening national security of individual states or the Alliance.

The importance and organisation of cyber security in relation to critical infrastructure is discussed by **Denis Čaleta** and **Gorazd Rolih.** They present the way this domain is regulated within the European Union, NATO and at the national level, as well as evoke certain deficiencies which are still to be dealt with.

Information security and its importance to the public administration are presented by **Maja Bolle** using the example of open-source and proprietary software. She acquaints us with their history and the way of functioning as well as the advantages

and disadvantages of opting for one of them. Of course, choosing either of them brings about numerous challenges, also discussed by the author.

Anže Rode, Kristian Beršnak and **Bojan Langerholc** present the Slovenian Armed Forces Special Operations Unit and its role within a wide national and transnational security context, putting emphasis on the potential crisis operations and possible co-unter-terrorism activities.

Zoltán Jobbágy and **László Szegő** have prepared a critical view of a generally well--accepted theory by Karl von Clausewitz. It has been tested with regard to the latest establishments based on the cases of Iraq and Afghanistan, while the authors also provided their personal reflections.

Original versions of the articles by Slovenian authors, which have been initially written in Slovene and later translated into English, are available in electronic version on the web page of Contemporary Military Challenges in a special appendix at the end of the publication.

This is our way of trying to reach out to a wide range of readers and potential future writers while respecting rational use of resources and quality indicators applicable to scientific and professional publications.

All our readers are kindly invited to write articles for our publication!

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.1

Ján Spišák

Strokovni članek

HIBRIDNE GROŽNJE IN RAZVOJ NOVEGA NATOVEGA SPLOŠNEGA KONCEPTA

HYBRID THREATS AND THE DEVELOPMENT OF THE NEW NATO OVERARCHING CONCEPT

Professional article

Povzetek Prispevek obravnava vidike novih varnostnih izzivov, ki jih vojaški teoretiki in avtorji varnostnih in obrambno-strateških dokumentov imenujejo hibridne grožnje. Trenutno so precejšnji izziv za zavezništvo in njegove interese. Hibridne grožnje vključujejo nasprotnike, vključno z državami, »malopridnimi« državami, nedržavnimi akterji ali terorističnimi organizacijami, ki lahko za doseganje svojih ciljev uporabijo različne kombinacije ukrepov v vse manj omejenem operativnem okolju. Hibridne grožnje so lahko kombinacija vseh vidikov vojskovanja ter skupek dejavnosti več nasprotnikov. Izkušnje iz trenutnih operacij so pokazale, da lahko nasprotniki zdaj izvajajo sovražne ukrepe s pomočjo številnih konvencionalnih ali nekonvencionalnih sredstev, metod in postopkov ter so pri tem uspešni, tudi če delujejo proti Natovim silam, ki so tehnološko in vojaško bolje podprte. Zavedanje razsežnosti in kompleksnosti prihodnjih groženj je zahtevalo razvoj splošnega sklepnega koncepta (Capstone Concept) za prispevek Nata k zoperstavljanju hibridnim grožnjam (*Military Contribution to Countering Hybrid Threats* – MCCHT. Ta koncept obravnava posebne izzive, ki jih predstavljajo trenutne in prihodnje grožnje, ter pojasnjuje, zakaj lahko ti izzivi od Nata zahtevajo, da prilagodi svoje strategijo, strukturo in zmogljivosti za naslednjih dvajset let.

Ključne besede ***Hibridne grožnje, hibridno vojskovanje, varnostni izzivi, koncept.***

Abstract This article deals with aspects of newly emerging security challenges that military theoreticians and authors of security and defense strategic documents name '*Hybrid Threats'*. They currently present a significant challenge for the Alliance and its interests. Hybrid Threats involve adversaries (including states, rogue states, non-state actors or terrorist organizations that may employ a combination of actions in an increasingly unconstrained operating environment in order to achieve their aims. Hybrid Threats may consist of a combination of every aspect of warfare and

compound the activities of multiple adversaries. Experience from current operations has demonstrated that adversaries can now conduct hostile actions through a broad array of conventional or non-conventional means, methods and procedures, having a favorable outcome against a NATO force that is technologically and militarily superior. Cognition of the scale and complexity of future threats has demanded a development of an overarching Capstone Concept[1] for the NATO *Military Contribution to Countering Hybrid Threats* (MCCHT). This Concept articulates the unique challenges posed by current and future Hybrid Threats and explains why these challenges may require NATO to adapt its strategy, structure and capabilities for the next twenty years.

Key words ***Hybrid threats, hybrid warfare, security challenges, concept.***

Introduction

Hybrid Threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives.[2]

Perhaps no country in NATO has dedicated so much effort in facing global security challenges as intensively as the United States. Representatives of the security community indicated an increase of various threats, which include traditional, irregular, terrorist or disruptive threats or challenges facing the state. This generates an unusual dilemma for today‘s military planners, whether to abandon the idea of preparing for war against state actors with conventional capabilities, or re-orienting for more likely scenarios of conflict with a non-state adversary using asymmetric operations and ‘irregular tactics’. At the same time they also recognize that both modes of actions can not exist separately.

A number of military theoreticians and strategists seek to discover and justify the existence of new forms of warfare, merging combined features of various types of military and non-military, combat and non-combat activities. They assume that future warfare will be hidden in the synergies, combining all the ways, methods and styles, which have been used to date. Their thoughts are turning to the „hybrid threats, „hybrid wars“ and „hybrid warfare“ and show that the combination will be used specifically against the weaknesses of their opponents. The particular challenges that were presented by separate philosophies of conventional enemies, terrorists or insurgents, converge in expectations of a collision with opponents that use all possible forms of violent actions. A part of the problem may even be criminal activities that destabilize local governments and/or encourage insurgents and foreign mercenaries, providing them with resources and assets, or undermining the authority of the host country and the legitimacy of its representatives.

---

[1] *MC 0583: A Capstone Concept is an overarching concept with the purpose of leading force development and employment primarily by providing a broad description of how to operate across significant portions of the complete spectrum of operations and describing what is required to meet strategic objectives.*

[2] *NATO agreed (31 May 10) see ref.: Internet sources [1]*

Hybrid Threats that sooner or later will be visible in hybrid warfare include, according to these theoreticians,[3] a whole spectrum of different aspects, including the capabilities of conventional, asymmetric, insurgent and terrorist acts and criminal activities. Hybrid wars can be waged between states and various non-state actors. They can be kept by separate units or even a single unit, operationally integrated and tactically incorporated and coordinated within the same operational area.

1 UNDERSTANDING OF MODERN THREATS

The origin of the term "hybrid wars" is often attributed to various authors. According to the one of the architects of the counterinsurgency doctrine, Dave Kilcullen, the first author who used the term "hybrid wars" was Erin Simpson who, during the conference for the Midwest Political Science Association (Chicago, April 2005) presented a paper *"Thinking about modern conflict: Hybrid wars, strategy, and war aims"*. According to Kilcullen, Simpson is the originator of this "extraordinarily valuable conceptual framework" (Kilcullen, 2008).[4]

Others offer Frank Hoffman, for his memoir *"Conflict in the 21st Century: The Rise of Hybrid Wars."* He states, however, that the credit for the first use of the term '*hybrid'* belongs to R. Walker who, in his unpublished doctoral thesis at the Naval Post Graduate School in Monterey, defined the Marine Expeditionary Unit as a *"hybrid force for Hybrid Wars"* back in 1998 (Hoffman, 2005).

Notwithstanding these and similar conjectures, one of the first provoking and certainly most inspirational thoughts inflaming the debate on the issue of hybrid wars, were those of General James N. Mattis and F. Hoffman, published in the U.S. Naval Institute Proceedings with title: *"Future Warfare: The Rise of Hybrid Wars."*. Mattis in his speech pointed out to the experience from Afghanistan and Iraq, highlighting the unexpected combination of technologies and methods of unorthodox tactical activities, that an unconventional enemy could use in the future. According to Mattis, so-called irregular challenges and methods of terrorism, fighting insurgents, unrestricted warfare, guerrilla wars or coercion by narco-criminals, will mostly likely represent the threats of the future (Mattis, Hoffman, 2005).

---

[3] *Beside authors cited in references see e.g. BIDDLE, Stephen., FRIEDMAN, Jeffrey A., 2008. The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy. Strategic Studies Institute, U. S. Army War College, Carlisle, ISBN 1-58487-362-0. EVANS, Michael., 2003. From Kadesh to Kandahar: Military Theory and the Future of War. Naval War College Review. SIMPSON, Erin., 2005. Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims. The Midwest Political Science Association, Chicago, Illinois. KILCULLEN, David., 2009. Accidental Guerrilla, New York: Oxford University Press. HOFFMAN, G. Frank., 2009. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. Washington, DC: Institute for National Strategic Studies, Strategic Forum 240.*

[4] *Based on D. Kilcullen´s blogging with Simpson in February 2008, regarding to paper, Thinking about modern conflict: Hybrid wars, strategy, and war aims.*

"We do not face a range of four separate challengers as much as the amendments to the combination of approaches - and manager of a different modes and means of war. This unprecedented synthesis is what we call Hybrid Warfare" (Mattis, Hoffman, 2005, p. 1).

Mattis continues that the war, which we will face in the future, is no longer just the General Krulak´s *'Three Block War'*. All aspects that must be taken into the account, Mattis characterized as follows:

"In hybrid wars we may face remnants of the fielded army of a rogue state in future wars, and they may employ conventional weapons in very novel or non-traditional ways. We can also expect to face unorthodox attacks or random acts of violence by sympathetic groups of non-state actors against our critical infrastructure or our transportation networks. We may also see other forms of economic war or crippling forms of computer network attacks against military or financial targets" (Mattis, Hoffman, 2005, p. 2).

The issues of hybrid wars are not only the mere deliberations of several military theoreticians. The United States National Defence Strategy (NDS) significantly expanded the understanding of modern threats. The previous mainstream of American thinking *"To fight and win the nation's wars"* which featured warfare against a conventional enemy, is heading toward a wide range of enemies that exist outside of the "traditional". The Strategy includes three other threats: irregular, terroristic and disruptive, that in the complex may usurp American power and hegemony through advanced technologies.

The Strategy assumed that the most complex challenges of the future might arise from the synergy of simultaneous applications of multiple methods of warfare (NDS, 2005). The Strategy even mentioned that the Department of Defence has invested too much into the traditional forms of warfare and there exists a need to shift resources and attention to other challenges. As Hoffman noted, National Defense Strategy and the "Quadrennial Defence Review (2006) well accepted that future challenges will avoid the U.S.'s unmatched power and seek alternative paths. *"We can no longer focus just on battles against preferred enemies"* (Hoffman, 2007, p. 9).

According to Hoffman, future scenarios will likely present a unique combination of synergies directed against Western society in general, and especially against the vulnerabilities of the United States. The future indicates that adversaries will be smarter than they are now and rarely restrict themselves in using only one tool available from the whole range of ways and methods that can be used simultaneously. Conventional, irregular and catastrophic-terrorist challenges will not be different and independent ways of warfare. All of them will be present in some form simultaneously. Mixing modes of warfare with a wide, diverse and complex range of technologies is *'hybrid warfare'* (Hoffman, 2007).

2 THE SOURCES OF THE NEW NATO´S CONCEPT

Before Hoffman published his ideas there were several military thinkers dealing with emerging threats. It is worth mentioning General Krulak´s famous prediction about the character of future conflicts, published by Robert Holzer in the Defence News article: *"Krulak Warns of Over-Reliance on Technology"*. According to Krulak:

"…future conflicts would be unlike the large-scale mechanized sweeps of Operation Desert Storm, but more like the "Stepchild of Somalia and Chechnya". The Chechens employed swarming tactics inside their own cities to thwart Russian domination. In Somalia, despite overwhelming superiority in firepower and technology, a group of lightly-armed 'rebels' effectively forced the US military out of the country by inflicting casualties on an elite unit" (Holzer, 1996, p. 4).

William Lind, one of the authors of the *Theory of Fourth Generation Warfare* in the article *"The Changing Face of War: Into the Fourth Generation"*, predicted in 1989 the nature of future threats. Lind says:

"... warfare seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point. It will be nonlinear, possibly to the point of having no definable battlefields or fronts. The distinction between 'civilian' and 'military' may disappear. Actions will occur concurrently throughout all participants' depth, including their society as a cultural, not just a physical, entity" (Lind, 1989, p. 2).

The 'Fourth Generation' concept has its opponents, such as the above mentioned General Mattis. For his own defence Lind, in another article *"Understanding Fourth Generation War",* tries repeatedly to explain the essence of the concept, citing Mattis, who, according to him, lacks the point of such warfare:

"Ultimately, a real understanding of history means that we face nothing new under the sun. For all the '4th Generation of War' intellectuals running around today saying that the nature of war has fundamentally changed, the tactics are wholly new, etc., I must respectfully say…'Not really… (Lind, 2004).

Later on, Lind accents on his own defence that the concept of 'Fourth Generation War' is not new, but represents a return to a method of warfare, that was waged before the establishment of the legal state as an institution.

"Now, as then, many different entities, not just governments of states, will wage war. They will wage war for many different reasons, not just "the extension of politics by other means." And they will use many different tools to fight war, not restricting themselves to what we recognize as military forces" (Lind, 2004).

Antulio J. Echevarria II is another determined opponent. He points out, in his article, *"Fourth-Generation War and Other Myths",* that what is being called 'Fourth Generation Warfare' is just insurgency. He also claims that the concept was '*discovered'* by Lind. Echevarria writes: *"The generational model is an ineffective way to depict changes in warfare. Simple displacement rarely takes place, significant developments typically occur in parallel"* (Echevarria, 2005, p. 10).

Although the theory of 'Fourth Generation War' has its opponents, it is obvious that it has provided a number of clues as to the development of hybrid threats and hybrid war concepts. The new concepts have also begun to address a broader community of experts. Many of them have brought more mature thoughts to the NATO overarching operating concept.

David. E. Johnson´s study paper, *"Military Capabilities for Hybrid War - Insights from the Israeli Defence Forces in Lebanon and Gaza"* is a part of an ongoing project – *"An Army for Full Spectrum Operations: Lessons from Irregular Wars"*. It represents one of the major contributions to the development of the *Hybrid Wars Theory*. Its objective is to evaluate current irregular and hybrid conflicts and their consequences for the U.S. Army, their capabilities and other forces supporting or operating with the Army. As current operations demonstrate, the Army is particularly important when fighting an enemy that applies irregular forms of warfare and where the claim *"to have boots on the ground"* (Johnson, 2010, p. 13) exists. The intention of the project is to *gain experience from the hybrid fighting of Israel's Defence Forces in Lebanon and Gaza*.[5] According to the project, insights into the operational context of warfare could bring information on the structure and capabilities of the forces that are exposed to hybrid threats.

3 HYBRID THREATS - FROM THEORIES TO THE CONCEPT

"The publication of this concept, based upon the leverage of on-going national thoughts and collaborative work with NATO and national Subject Matter Experts, focuses on outlining the challenges posed by hybrid threats and provides an initial framework for countering them." 6

Alex Smethurst, ACT lead analyst on the concept

One of the primary sources that justify the existence, scope and complexity of both conventional and unconventional future threats, was the final review of Allied Command Transformation (ACT) from the project *"Multiple Futures Project" (MFP)*. The International Military Staff (IMS) ordered in consequences, that both strategic commands will initiate the development of the new overarching concept

[5] *For a similar study from the conflict between IDF and Hezbollah see: BIDDLE, Stephen., FRIEDMAN, Jeffrey A., 2008. The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy. Strategic Studies Institute, U. S. Army War College, Carlisle, ISBN 1-58487-362-0.*

[6] *http://www.act.nato.int/multimedia/archive/41-top-headlines/464-act-sees-progress-on-countering-hybrid-threats-concept*

for the resolution of hybrid threats. The analysis of major strategic documents (directives, doctrine, research reports, etc.) was conducted by strategic headquarters, national representatives, NATO Centres of Excellence (COE) and the other partners.

The crucial role in developing the new concept pertains to the *Counter Threat Hybrid Integrated Project Team* which, since the beginning of 2009, has dealt with issues of hybrid threats assessment. The team created a detailed plan for the evaluation of hybrid threats and broader challenges. Since then it has made a number of international workshops conducted by ACT, where numbers of representatives from both member and non-NATO nations are present, helping to develop the concept.

The reality of the possible advent of hybrid threats has become an important issue for political and military leaders of NATO. Half of the year 2010 brought a number of activities that have contributed to the draft development of the new NATO operating concept "*Military Contribution to Countering Hybrid Threats" (MCCHT)*. ACT conducted a detailed analysis of the security environment, created and published (August 2010) the first draft of the concept dealing with many problems and challenges that may affect the existence of NATO over the next two decades. Many of the key issues were then raised during the NATO summit in Lisbon (November 2010) and in the concluding declaration of the participating Heads of States and Governments.

The proposed draft highlights three important issues. Firstly, while the contemporary NATO policy, strategy and doctrinal framework remain valid, there are new areas of threats, which may expand beyond the current horizon. Secondly, the division between military and civilian responsibilities in the changing security environment is becoming more difficult to define and thirdly, the Alliance will require much more collaboration and partnerships beyond its existing scope.

The draft of the new concept identifies the emerging challenges and addresses them with the term 'hybrid threat'. It describes how these threats manifest themselves and provides an estimate of how NATO could contribute to manage them. There are serious considerations about cyber attack, energy security, terrorism, international crime, lack of strategic resources and the increasing commercial availability of lethal technologies and materials. With regard to emerging security challenges, the draft of the concept provides the key implications for NATO and offers some possible solutions in facing them.

The document stresses the Alliance's obligation in strengthening its own capability and to act against hybrid threats comprehensively. Their complexity requires a holistic approach and the ability to respond in conjunction with the broad international community. In some aspects the individual countries could count on taking over the leading role in the fight against the threat with the support of the NATO military component. Hybrid threats will have a tendency to exploit the gaps in the security environment across the spectrum of conflict. NATO should hence enhance cooperation with other organizations to respond to any threat effectively.

4 COUNTER HYBRID THREATS EXPERIMENT – A WAY AHEAD

The USJFCOM Joint Irregular Warfare Centre (JIWC) provided significant help to execute the ACT experiment *"Counter Threats Hybrid Experiment"*[7] in May 2011. Rather than being based on formal policy, it was taken more as an intellectual forum in which individual participants analyzed, discussed and better understood the complex set of issues facing NATO and the wider community to address the new security challenges. The main purpose of the experiment was to find and discuss the critical implications of proposals for the new concept and to elaborate possible approaches to solving the critical issues. The experiment has attracted the attention and participation of not only NATO member states, but also representatives from academia, business and international partners. One of the key outcomes of the experiment was to provide a clear recommendation to the political and military leadership of NATO, about what this organization must do to support the broad international community in coping with a set of hybrid challenges. The results of the experiment were directly taken into account in subsequent development and refinement of the concept. It is assumed that the final product – *Military Contribution to Countering Hybrid Threats* – will be finished at the end of 2011.

Conclusion

Even though a draft, this concept offers a careful analysis of the evolving security environment in which NATO will have to react. It is obvious that the complexity of future challenges will require adjustment of NATO's structures, processes and capabilities in several key areas to be effective. Any response of NATO will likely depend on aspects outside the existing scope of NATO's military community and may be particularly problematic especially with regard to the issue of cooperation with non-military agencies and a thorough understanding of the civil-military interface needed to achieve unity. It will therefore be necessary to consult the issues with representatives of the political sphere. Political consensus among NATO member states in the region (beyond purely military involvement), has remained an important issue, as well as dealing with the consequences of rapid technological development.

Authors of this concept are aware that further development is based on the current restrictions. It is also a matter of sensitive intellectual debate about the future security challenges beyond a rigid paradigm. They assume both further follow-up discussions on new hybrid threats and sophisticated decision-making, in which the Alliance will need to transform.

[7] *For all the agenda concerning the experiment, relevant documents and activities, see: https://transnet.act.nato.int/WISE/ACTIPT/JOUIPT/20102011CH/Experiment*

Bibliography

1. *BIDDLE, Stephen., FRIEDMAN, Jeffrey A., 2008. The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy. Strategic Studies Institute, U. S. Army War College, Carlisle, ISBN 1-58487-362-0.*
2. *ECHEVARRIA, J. Antulio II., 2005. Fourth-Generation War and Other Myth. Strategic Studies Institute, U. S. Army War College, 122 Forbes Ave, Carlisle, PA 17013-5244.*
3. *EVANS, Michael., 2003. From Kadesh to Kandahar: Military Theory and the Future of War. Naval War College Review.*
4. *HOFFMAN, F., 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 72 p.*
5. *HOFFMAN, G. Frank., 2009. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. Washington, DC: Institute for National Strategic Studies, Strategic Forum 240.*
6. *HOFFMAN, G. Frank., 2009. Hybrid warfare and challenges. Joint Force Quarterly, p. 34–48.*
7. *HOLZER, Robert., 1996. Krulak Warns of Over-Reliance on Technology. Defense News, p. 7-13.*
8. *KILCULLEN, David., 2009. Accidental Guerrilla, New York: Oxford University Press.*
9. *McCUEN, J. John., 2008. Hybrid Wars. Military Review, p. 107–113.*
10. *SIMPSON, Erin., 2005. Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims. The Midwest Political Science Association, Chicago, Illinois.*

Internet sources

1. *https://transnet.act.nato.int/WISE/CollaboCat/ACTIPT/JOUIPT, 16 August 2011.*
2. *https://transnet.act.nato.int/WISE/ACTIPT/JOUIPT/20102011CH/Experiment May 2011. 10 May 2011*
3. *JOHNSON D. E., 2010. Military Capabilities for Hybrid War - Insights from the Israel Defense Forces in Lebanon and Gaza. RAND Corporation, Santa Monica, 20 p. ISBN 978-0-8330-4926-1. http://www.rand.org/pubs/occasional_papers/2010/RAND_OP285.pdf, 10 May 2011.*
4. *LIND, William., NIGHTENGALE, Keith., SCHMITT, John F., SUTTON, Joseph W., WILSON, Gary I., 1989. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, p. 22-26. http://twm.co.nz/4thgenwar.htm, 6 April 2011.*
5. *LIND, William., 2004. Understanding Fourth Generation War. http://antiwar.com/lind/index.php?articleid=1702, 12 April 2011.*
6. *MATTIS, James N., HOFFMAN, Frank., 2005. Future Warfare: The Rise of Hybrid Wars. Naval Institute Proceedings Vol. 132, No. 11. http://www.usni.org/magazines/proceedings/2005,18 April 2011.*
7. *National Defence Strategy, 2005. Washington, DC: U.S. Department of Defence. 25 p. http://www.defense.gov/news/Mar2005/d20050318nds2.pdf, 20 April 2011.*
8. *SACT MULTIPLE FUTURES PROJECT FINAL REPORT, 2009. 195 p. http://www.bits.de/NRANEU/nato-strategy/20090503_MFP_annexes.pdf, 18 May 2011.*

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.2

Uroš Svete,
Anja Kolak

Izvirni znanstveni članek

VARNOSTNA RELEVANTNOST KIBERNETSKEGA PROSTORA V OBDOBJU WEB 2.0

CYBERSPACE SECURITY RELEVANCE IN THE TIME OF WEB 2.0

Original scientific article

Povzetek Informacijska tehnologija in varnostni sektor sta bila vseskozi povezana, še posebej pomembna pa je razprava postala v času, ko so praktično vse ključne družbene infrastrukture postale odvisne od digitalne tehnologije. V tem članku smo z uporabo varnostnih teorij analizirali pomen kibernetskega prostora, pri čemer smo posebno pozornost namenili razvoju druge generacije svetovnega spleta (in v tem okviru posebej primera WikiLeaks, pri katerem so nosilno vlogo pri proizvodnji podatkov in informacij prevzeli uporabniki sami. Internet je tako res postal komunikacijska hrbtenica, prek katere so povezane množice uporabnikov, tako komuniciranje pa (zahodnim) državam predstavlja vse večji izziv, včasih celo grožnjo njihovi nacionalni varnosti.

Ključne besede ***Informacijsko-komunikacijska tehnologija, kibernetski prostor, sekuritizacija, Splet 2.0, WikiLeaks.***

Abstract Regardless if the information-communication technology has been developed to follow national security interests or not, at the moment, nobody doubts this correlation anymore. But the discussion has become much more important in time when practically all critical social infrastructures and processes depend on digital technology. In the paper, importance of the cyberspace has been analysed by security theories and with special focus on the Web 2.0 and WikiLeaks issue. The current way of such interactive communication is namely based on individuals as data and information producers, which could be in (Western countries perceived as a greater challenge and in some cases even national security threat.

Key words ***Information and Communication Technology, cyberspace, securitization, Web 2.0, WikiLeaks.***

Introduction

Throughout human history, technological and technical revolutions have also had security dimensions. However, none of them have changed the power relations in a way the information and communication technology (ICT) and related information revolution has. We often think that the Cold War period was mainly marked with (nuclear) arms race and war for resources in a physical (real) space[1]. However an increasing number of authors have looked for reasons for a well-known result of this era and the supremacy of the western world[2] within the development of information technology and its impact of weapons systems as the ways of the functioning of military and non-military organisational structures (Štrubej, 2008, Klimburg, 2011). Despite varying explanations of the reasons and intentions which had resulted in the predecessor of Internet, ARPANET[3], there is today broader consent on the fact that the expansion of ICT and the appearance of cyberspace[4] have undoubtedly fundamentally changed practically all social subsystems as well as the role of an individual in them. Regardless of how we estimate the developments in late 1950s and early 1960s which have resulted in the informatisation of the world, there is no doubt that cyberspace and security sector have been connected from the very beginning, both in theoretically conceptual and empiric sense. Their relation has been inversely deductive throughout the process. The development of technological capabilities and components has inspired theoreticians (think-tanks) for developing the concepts. However, an inverse relationship is also in place, where several information and cyber operations ideas and concepts have only appeared recently. Although in the recent decade, there has been much writing on ICT security implications in Slovenian scientific and professional world as well, this paper would like to emphasize some new effects characterised for digitalised society. Main focus will be put on the part of the cyberspace development called Web 2.0 as well on security-oriented discussions mainly related to the developments concerning the WikiLeaks "affair". The latter has brought attention back to an individual user and making ICT a real socially technical network (Kling, 2000), where *we're living through reverberations in the form of numerous social media sites and activities that have contributed to nontrivial changes in how w*e learn, play, socialize, entertain, engage with our governments (Davis, 2011, p. 92). On the other hand, it has also underlined the dialectics which

---

[1] *In 1948, international relations theorist, Hans Morgenthau (1904–1980) theorized that national security depends on the integrity of a nation's borders and its institutions (Morgenthau in Geers, 2009, pp. 1).*

[2] *Unlike the American planners who saw the US military benefiting from this silicon revolution, the Soviets were worried about their own economic inability to exploit the digital revolution. The USSR was rapidly losing ground to US prowess in microelectronics (Hughes, 2010, pp. 527).*

[3] *Charles Herzfeld, ARPA Director (1965–1967) argued The ARPANET was not started to create a Command and Control System that would survive a nuclear attack, as many now claim. To build such a system was, clearly, a major military need, but it was not ARPA's mission to do this; in fact, they would have been severely criticized had they tried. Rather, the ARPANET came out of our frustration that there were only a limited number of large, powerful research computers in the country, and that many research investigators, who should have access to them, were geographically separated from them (http://arpanet.co.tv/).On the other hand, Štrubej (2008) sees main initiators of developing the aforementioned network in the tendency to establish a control and communication network capable of surviving a nuclear attack.*

[4] *Cyberspace is the electronic medium of computer networks, in which online communication takes place. The world was first used by William Gibson (http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317) and cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content (Deibert and Rohozinski, 2010a, p. 16).*

was unimaginable in early 1960s – the very contradiction between a state and its citizens, which nowadays mainly reflects in asymmetry (disagreement) of security concepts, instruments and interests. The example of WikiLeaks is not the only one related to the security of information networks or computer security in a narrow sense. We consider it just as a beginning of the battle for control over ICT users, which will in the future be led by states, non-state (commercial) actors and groups of people with good information technology ability and awareness. Another example, which has in the recent time undoubtedly captured attention, is the ability of destructive use of ICT, which threatens the functioning of critical social infrastructure[5] even when it has no direct access to the Internet. Such case is Stuxnet worm which mainly affected industrial facilities using Siemens Win CC or PCS7 software. It activated itself only if computers were fitted with the mentioned software, which makes it obvious that the aim was not to target a wide circle of usual users, but specific industrial facilities (W32.Stuxnet Dossier, 2011)[6]. Both of the mentioned examples prove that cyberspace is really gaining strategic importance, both, by directly influencing our perception of the environment (also in the sense of security) and by fundamentally changing the functioning of traditional security actors.

Even though, in Slovenia, such discussions used to be perceived with mistrust, scepticism or even ridicule, such realistic examples of cyberspace threats, its influence of the redistribution of social power and, last but not least, the inclusion of the issue in the NATO's New Strategic Concept and the work of the EU[7] force us to seriously address this issue, both, academically and within state authorities and not to keep it just on the paper at the highest strategic levels[8]. Estonia is a good example of how cyberspace perception is not (always) related to financial resources and how even small countries can establish themselves as information security agenda setters.

1 CYBERSPACE IN A SECURITY DISCUSSION

From the very beginning, cyberspace and ICT in general have been closely related to the (national) security sector. However, more precise concepts were not developed until several decades later, when ICT entered practically all social spheres.

---

[5] *Critical infrastructure owners and operators report that their networks and control systems are under repeated cyber-attack, often from high-level adversaries like foreign nation-states. And these kinds of attacks on critical systems such as gas, power and water have increased around the world in last few years (In the Crossfire Critical Infrastructure in the Age of Cyber War, 2009).*

[6] *Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or (nuclear) power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries. Stuxnet was discovered in July, but is confirmed to have existed at least one year prior and likely even before. The majority of infections were found in Iran (W32.Stuxnet Dossier, 2011).*

[7] *OPINION of the European Economic and Social Committee on the 'Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (2011).*

[8] *Nevertheless, it is commendable that cyber threats and abuse of information technology and systems have been explicitly mentioned in the latest Resolution on the National Security Strategy of the Republic of Slovenia ReSNV-1, 2010).*

Although top authorities of the US Department of Defense were aware of the significance of information technology and its role in Revolution in Military Affairs[9] as early as in 1960s and 1970s, more precise information warfare concepts had not been developed until a while later (Hughes, 2010). New strategies and tactics for the pursuance of their aims have been described under the umbrella term 'information warfare'. Although the doctrine of information warfare has emerged from work by researchers and military strategists of the RAND Corporation (Arquilla and Ronfeldt, 1999), it has been used to describe the strategic transformation of the network society also by other kinds of thinkers including social critics, computer scientists (Denning, 1998), business strategists (Munro 2009) and political theorists (Der Derian, 2000). The US approach to the so-called strategic evaluation of ICT has from the very beginning been very defence- and military-oriented. However, it has involved technical personnel as well as social science experts and it has soon been established that strategic use of ICT will have to involve more than just the civil society.

The weapons of information warfare have been developed and refined in both the military and civilian realms of society. Indeed, the theorists of the RAND Corporation note that with information warfare the military and civilian realms have become blurred. The doctrine of information warfare is somewhat broader and more ambitious than simple misinformation and propaganda, although these latter techniques have an important place in the information warfare arsenal. Information technologies and communications networks are the weapons and the targets of information warfare operations. Techniques of information warfare can involve both high and low technology weapons, but it has only emerged as a distinct doctrine in association with the use of relatively hi-tech equipment such as computers, satellites and the Internet. The range of hi-tech weapons includes techniques such as computer viruses, hacking, identity theft, email bombs, phishing and the creation and destruction of websites. Low-tech weapons have been described by the hacker Kevin Mitnick as 'social engineering', but may also include more mundane aspects of social life such as pamphleteering and the spread of rumours. In short, it uses information to undermine and disorientate an adversary, disrupting their ability to effectively mobilize their resources (Munro, 2009, p. 200). In the recent period, USA go even one step further and according to some reports the US is set to publish plans that will categorize cyber-attacks as acts of war against US. In future, a response to a cyber-incident or attack on the US critical infrastructure would not necessarily be a cyber-response. All appropriate options would be on the table and a US president could consider economic sanctions, cyber-retaliation or a military strike if key US computer systems were attacked (Pentagon to treat cyber-attacks as 'acts of war', 2011.)

[9] *In the early 1970s the innovative thinker Andrew Marshall was recruited from the RAND Corporation (Research and Development) by the US Department of Defense to head its Office of Net Assessment. At the Pentagon, Marshall was given the tall-order task of finding ways for NATO to defeat the Warsaw Pact short of a nuclear response. In his first departmental report Marshall told of the progress that US weapons labs were making on a new generation of 'smart' weaponry that would deliver substantially increased lethality with a lower loss of US life. The increased precision was made possible by a new generation of software and electronics built around the microprocessor (Hughes, 2010, pp. 526-527).*

While the number of ICT users grows and ICT is becoming gradually demonopolised and commercialised, the concept of information warfare is becoming increasingly focused on offensive and defensive operations of armed forces. However, there is, on the other hand, a concept of (strategic) cyberspace and its defence, since people and their ideas and knowledge have truly become an integral part of information and communication technology[10]. Security discussions have split in this respect as well.

Taking note of what has been said over the past few years about the mission of computer security, two conceptions seem dominant. One, here labelled ‘‘technical computer security,’’ has its roots in the scientific and technical field of the same. The other, here labelled ‘‘cyber-security,’’ a more recent entry to the public sphere, is typically articulated by government authorities, corporate heads, and leaders of other non-governmental sectors. It links computer security to traditional notions of national security. At present, these two conceptions exist side-by-side, each one angling for the attention of key social actors including government agencies, technical experts and institutions, corporations, policy experts, pundits, the general public, and, importantly, the media (Nissenbaum, 2005, p. 63). On the other hand, the term ‘cyber warfare’ is used to indicate broadly any warfare waged by states and significant non-state actors in cyberspace. It can include defending information and communications systems, critical infrastructures, weapons systems or military command centres from attack, as well as conducting equivalent offensive operations against an adversary. It does not refer to recreational or socially motivated hacking or ‘hacktivism (Hughes, 2010, p. 525).

If, on the one hand, the US view of cyberspace from a security perspective is still more or less state-centric and realistically oriented in a defence and military sense[11], we cannot avoid the Copenhagen school across the Atlantic and the third (critical) perspective of dealing with modern security issues. The latter is particularly important for our discussion, because it considers two extremely important changes also caused by the informatisation of modern societies. The first one is greater particularisation of security interests and lack of unity between a state and its citizens, while the second one is the complexity of modern security environment. Both can, in our opinion, be understood only if we are precisely aware of social consequences of informatisation which nowadays includes at least half of all humankind.

In proposing a constructivist framework, Buzan and Waever are less concerned with providing an objective characterization of threats, vulnerabilities, and modes of defence, and more with providing a systematic account of the ways specific conditions, states-of-affairs, or events are posed by significant social actors as threats to

---

[10] *Crowdsourcing as a concept as well as a practice refers to the idea that the Web can facilitate the aggregation or selection of useful information from a potentially large number of people connected to the Internet. Wikipedia and, more recently, WikiLeaks are good examples of this distributed knowledge gathering and organization in action (Davis, 2011, p. 92).*

[11] *We are, of course, aware that, in pursuit of this aim, the US is trying to mobilise all social resources. This »whole of nation« approach to security policy – the joint integrated application of state (whole of government) and non-state (business and civil society) efforts to attain common objectives – has only recently begun to be applied in US government circles (Klimburg, 2011, p.43).*

security and come to be widely accepted as such. They call this rendering of a security threat ‘‘securitization,’’ which becomes the fundamental explanatory construct of their framework. The concept of securitization generalizes certain elements of traditional approaches to national security in which the typical landscape includes a threat of military attack, the nation-state under threat, and the specific steps leaders take to ensure the state’s continued security (through such means as defensive action, shoring up vulnerabilities, and so forth.) The Copenhagen School moves from this landscape to the one in which the threat need not be military and the referent object need not be the state (Nissenbaum, 2005, p. 66).

1.1 FROM NATIONAL AND STATE TO HUMAN SECURITY APPROACH

The next very important theoretical framework for understanding security relevance of nowadays cyberspace is also a move and spreading of security actors and threats as well. Instead of the fact that traditional security threats have been rearticulated, the following debate allowed also for treating cyber threat as a constitutional part of modern security at national as well as individual, and even international level.

The (national) security overview in recent decades has shown the prevalence of two main approaches in particular: the traditional (deterministic) and post-modern (complex). For the first, security is the absence of an external threat, or better put, military means should be used for confronting (external) threats. This approach justifies national security as a legitimate way for organizing violence within or between states, but not in any case beyond that (Malešič, 2004). The state has a central role in these security debates; on the other hand it ensures its security interests within the framework of an anarchic and hierarchic international environment, above all using military means or military power (Waltz, 2000). In this sense a traditional security approach is typically realistic. It prevailed during the Cold War and was a theoretical base for simplistic, but very important explanations of wars, alliances, imperialism, blockades and other important international topics (Walt, 1998).

The other main concepts, developed in the Cold War period and based on the starting points mentioned, are common security, stable peace and security approaches in the Third World. Although these concepts go beyond our discussion, they have some very important implications for moving security attention from the state to an individual level. While the common security project was the outcome of political élites, the stable peace concept arose from academic research of peace, based on Galtung’s and Boulding’s analyses. In this sense, peace could not be considered as the absence of war but as a state of society, which ensures the requisite conditions of social justice. Therefore Galtung (Bilgin, 2003, p. 204) differentiates between personal and structural violence. Equally, he divides negative peace as absence of armed conflicts from positive peace as absence of direct (physical) and indirect (structural and cultural) violence. To achieve positive peace, dialogue, cooperation and solidarity among peoples have to be re-established. It is understandable that Galtung and other authors redirected research focus from the state and military dimension towards individuals and social groups (Bilgin, 2003, p. 204-205).

In the 1960s, more complex definitions of national security appeared. According to the liberal and especially the constructivist critical security theory, the foci and security agenda had moved from the national state level towards non-state actors. But the new security understanding ("new security") did not acquire significant legitimacy until the end of the Cold War, when human beings/individuals as reference objects of security had been exposed to the collapse of the static bipolar world order and influence of the globalization (the concept of human security) (Newman, 2001). On the other hand, the legitimacy of discussion about security subjects (whose security?), security emancipation and insecurity dilemmas (butter or guns, individual vs. state/nation etc.), as well as societal/human security and risk society, is increasing significantly. These can be paraphrased or described by social development trends such as growing economic and political inequalities within particular national states as well as between them, a lack of natural resources, migration problems, the spreading of intrastate conflicts, undermining of international peace and stability, and technological challenges. These are just some of the agenda-setting issues or issues that traditional security paradigm is not in position to face. Within this framework, more complex security definitions should be understood (Bilgin, 2003). Security – whether or not one insists on a distinction between 'hard' and 'soft' security – is about more than protecting a country from external threats; security may well include critical infrastructure protection, economic, social security, environmental and human security (Liotta, 2002, p. 475). Security is therefore a matter of feelings and a matter of our physical environment perception.

Following thesis may be too bolt, but without informatisation, the decentralisation of modern societies would not be as fast and it is a big question, if the societies had even wanted such way of social development. While self-initiative and private initiatives in the US have been crucial for the development of ICT, individualisation has also significantly changed security perspectives. Since security implications of ICT can be divided into direct ones (when the use of ICT makes changes in the perception of reality and, consequently, threat) and indirect ones (working of traditional security instruments and mechanisms has been changing by the use of ICT) (Svete, 2005), it is completely understandable why such a large concept and theory apparatus is needed. This is particularly true with regard to the security analysis of the part of ICT development, which we call Web 2.0 and which will logically be followed by the Internet of Things, when, in addition to the humankind, practically all electronic devices will be interconnected[12]. If, in the initial phase, the Internet was complex merely due to its technical component enforcing the principle of decentralised action, the second phase is linked to complexity arising from the transformation of millions of ICT

[12] *"A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communications capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent federated services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability." (CASAGRAS, an EU Framework 7 Project, 2009). The evolving vision of Web 3.0 (sometimes referred to as the service Web) is based on the balanced integration of diverse services provided by human agents and machines over the World Wide Web. This is also the intuition that drives crowd-servicing, which lets us create platforms on which we can build new applications and even enterprises (Davies, 2011, p.93).*

users from readers, spectators and listeners of electronic media into active users and producers of multimedia information capable of real-time transfer and use. Davis (2011) in such cases uses the term 'crowdsourcing' denoting users (the crowd) as the main source of information.

2 CYBERSPACE COMPLEXITY AND SECURITY DILLEMA IN WESTERN DEMOCRACIES

As it has been mentioned, cyberspace is a global and extremely complex web of electronic devices and users with Internet access having a wide variety of aims and interests. It is therefore completely logical that the reaction to providing of security, both from a national and individual perspective, has to be complex and comprehensive. But is this really the case?

Although, in theory it is clear enough that the cyber security problem does not fit conventional or traditional security categories based on individual security responsibilities, economic or corporate security issues, military security problems, as well as domestic versus international problems, the practice is not so concise. Hence, domestic law enforcement must interface with military defence information warfare operators. In addition to that, cyber security is non-geographic; therefore the notion of territorial divisions of responsibility makes little sense. Computerized information flows around the world, investigators of each country like the Federal Bureau of Investigation or other national polices must thus increasingly cooperate with foreign law enforcement agencies to solve cybercrimes[13] (Harknett and Stever, 2011, pp. 455-456). There have, however, been several attempts, especially at a national, but also international level, using reformed and adjusted, but still traditional security mechanisms to deal with contemporary challenges. And at that point we notice the entire scope of different concepts of, both, cyber threats as well as corresponding responses. Deterrence, civil defence, collective defence, and arms control were key national security doctrines in the 20th century, and they are being revaluated now for application to cyberspace (Michael, Tikk, Wahlgren, Wingfield, 2010, p. 91). But is this even possible? As it will be evident later on (especially in the case study on WikiLeaks and the responses to it), it was especially the western countries that found themselves in a great dilemma. On the one hand, they have been accelerating the development and dispersion of information technology for several years, trying to obtain world supremacy in economy, politics, culture and security. For western democracies, the most important dimension of cyber power is thus the ability to motivate and attract their own citizens, an inward focused soft-power approach that is fundamental for creating "whole of nation cyber capability (Klimburg, 2011, p. 43). On the other hand, their critical infrastructure is becoming increasingly dependent on ICT. Considering the fact that we have recently witnessed a vast increase in threats to information critical infrastructure posed, both, by other countries and individuals

[13] *As an example we can put out also Maribor's group of crackers (computer criminals), responsible for developing a virus that breaking into credit cards numbers and other confidential data made possible. This case was investigated by FBI and Slovenian police.*

(whose interests may be purely personal or who may for various reasons link up at an international level), it is perfectly logical that cyber security has become a common topic in lay, professional and political public. There is no more doubt that cyberspace access has grown to become a national security concern in most nations because of the integral role that information and communication technology (ICT) plays in most aspects of private and public affairs. Actions against this critical infrastructure can be criminal, requiring a law enforcement response; involve espionage, which demands action by a country's intelligence community; or even come in the form of an armed attack that permits military self-defence by a nation's armed forces (Michael, Tikk, Wahlgren, Wingfield, 2010, p. 91). In this respect, it is interesting that an increasing number of cyber security initiatives see solutions in an international agreement and cooperation among countries. In today's interconnected networks, (cyber) threats can originate anywhere. Therefore national, regional and international co-operation and coordinated action is needed to address cyber security-related issues (Sund, 2007, p. 571). Hughes (2010) proposes that a multilateral regime is needed to govern cyber-warfare at the global level. As the prospect of a prolonged interstate cyber-war increases, this article examines the role that a cyber-warfare treaty or 'Treaty for Cyberspace' could play in limiting the adverse human effects of interstate conflict in cyberspace. Without this kind of consensus the world may indeed be witnessing not only the rise of a new zone of strategic competition but, more consequentially, ground zero for the next global arms race[14]. Such kind of proposals have been supported also by Geers (2010b) who's idea is Cyber Weapons Convention according to good results brought about by 1997 Chemical Weapons Convention (CWC). The aforementioned approach is therefore trying to respond to cyber threats with an international agreement as an instrument of collective security which would limit or even inhibit the arms race in cyberspace. A problem arising thereof is a technical or legally normative limitation of users' freedom which has throughout the process been the motor of ICT development.

The second interesting example is the securitisation of cyberspace and threats within NATO, which should transform from a Cold-War form (1.0) into a second-generation security organisation (2.0). The widely publicized attacks on Estonian networks in 2007 and Georgia's state systems in 2008 have been attributed either to Russian patriotic hackers or to official Russian agents. NATO responded to the Estonia network shutdown by convening an emergency meeting of the North Atlantic Council; and at the 2008 Bucharest summit, the alliance announced its first cyber-defence policy, marking the first occasion on which an international military organization had deemed cyber-security to be a collective defence obligation. NATO claims that, should a member state face a catastrophic cyber-attack, its new cyber-security

[14] *By the start of 2010 China, India and Russia alongside the US, the UK and South Korea are among the first group of countries to establish formal command and control (C2) over military assets in the cyber-domain. In addition, a host of non-state actors are engaged in cyber-warfare. Al-Qaeda, Hezbollah, Hamas, Zapatistas and a variety of 'patriotic' hacker-attackers are just some of the known paramilitary, resistance or revolutionary groups that have used cyber-warfare or plan to engage in it, with or without specific state sanction. As numerous media accounts have attested, even a teenager armed with a consumer PC and a broadband connection can wreak havoc on both business and government organizations in cyberspace, as demonstrated in 1999 by teenage British hackers who altered British military secure satellite orbits (Hughes, 2010, p. 524).*

policy gives it the tools to respond effectively (Hughes, 2010, p. 529). Also Myrli (2011, p. 87) found out the cyber threats become global therefore every successful security mechanism would need cooperation. But at the same time he is aware of complication factors. Much of the vulnerability to cyber-attack stems from a lack of preparedness in both the governmental and private sectors. Over 50% of industry insiders and other experts from the US, Europe, and Canada said that utilities, oil and gas, transportation, telecommunications, chemical, emergency services, and postal/shipping industries were not prepared for a cyber attack. However, the anonymity enjoyed by cyber aggressors adds a deeply complicating dimension to the nature of the threat. Unlike the telephone system, which has an effective tracking and billing capability based on the need to charge users, the Internet was designed as an open and robust system for the sharing of information, and therefore has no standard provisions for tracking or tracing the behaviour of its users. And last but not least competition exists. Though emerging threats to some extent could compel players to cooperate, the global security situation is still complicated as nations or blocs are vying mainly for their own benefits. The case is the same with NATO. While claiming that it does not consider any country to be its adversary, NATO still puts deterrence as a core element of its overall strategy.

The challenge of cyber security is both significant and complex. Achieving effective regulatory governance in this area calls for a comprehensive strategy that involves coordinated action by government, the private sector, and individual citizens. Of course, an undertaking of this size and magnitude cannot be completed overnight – it requires a sustained, multi-year effort with significant governmental and private sector cooperation (Chertoff, 2008, p. 484). However did we already reach such kind of security development? More likely, we could concur with the finding of Deibert and Rohozinski (2010b, p. 44) that pointed out rather than being an ungoverned realm, cyberspace is perhaps best likened to a gangster-dominated version of New York: a tangled web of rival public and private authorities, civic associations, criminal networks, and underground economies. After all, this establishment is also supported by dilemmas relating to the provision of information security, which increasingly appears to be the victim of discrepancy between state interests and specific interests. In this respect it is more than obvious that mainly western democracies somehow have problems determining the boundary between the freedom of ICT use and the threat to (national) security. The USA and many other western democracies thus, on the one hand, support informational freedom in the countries like China, Iran and Arabic countries, mainly in the use of the second-generation social networks on the World Wide Web, but on the other hand limit this very freedom, when their national security and strategic priorities are threatened. It is this dilemma that we find as one of the crucial ones to impact further ICT development. In a technical sense, this web will be much harder to control, especially after the transfer to the Internet Protocol version 6, because the number of connected devices will increase rapidly. In the end, it will be possible to achieve information security only by physically disconnecting the network, which some dictators in Arab countries have already attempted. And we know how they ended up. Since in such events, the mobilisation power of

social networks and their influence even on social processes became evident, we will focus more on the second-generation web and the Wiki platform which started a real "cyber war" between its supporters and opponents. There is, however, one other important dilemma supported by Deibert and Rohozinski (2011). They draw attention to the fact that, in the information age, we leave digital traces practically everywhere, copying our analogue lives into the binary code. Digital information can easily be tracked and traced, and then related to specific individuals who themselves can be mapped in space and time with a degree of sophistication that would make the greatest tyrants of the past days envious. So, are these technologies of freedom or are they technologies of control? This goes especially for the rise of social networks, such as the Facebook, and the platforms abiding by cloud computing (Google, Apple, Microsoft). And, in terms of their value and influence, these brands belong to the top companies, at the same time shining out the cyber power of the USA, which its main allies, competitors and opponents are well aware of.

2.1 THE SECOND-GENERATION WEB

In contrast to the first generation of the development and use of the Internet, which was mainly used in the same manner as the traditional media (characteristic of them is a one-way data flow), the biggest revolution occurred with their engagement and cooperation in the development of services and their contents. Web 2.0 thus benefits from the biggest advantage of the Internet infrastructure, i.e. its interactive use, which of course requires an active user.

The most significant characteristics that a core 'Web 2.0 service' follows (http://www.techpluto.com/web-20-services/):

- **User-centred Design**. A web design which is created in a way that it fulfils every possible need of the end user and empowers the user to perform certain customizations within the design. User-centred designs are cleaner, often Ajax based and easy to navigate. The appearance of the design is given a special preference while creating such a design. iGoogle, a customizable Google homepage is one of the most appropriate examples of a User-centred design.
- **Crowd-sourcing**. Every small unit of contribution is important to a Web 2.0 service. Millions of such contributions eventually lead the website to state of higher relevance. For instance, any conventional Media company (employing hundreds of reporters) has today been easily beaten by blogging platforms like Blogger and WordPress in producing extremely frequent and relevant content as millions of users are acting as a contributor, building up a large resource within much lesser span of time.
- **Web as Platform**. Gone are those days when one had to heavily rely on the desktop for accessing various web applications. Today's Web 2.0 services don't require a client download condition. Nor is the dependency on a particular OS for accessing the web services. Whatever be the method of internet access (Windows, Mac or Mobile OS), the Web 2.0 applications are nowhere affected by it.
- **Collaboration**. Wikipedia takes the first place when it comes to proving the power of collaboration. Before 2001 (year of Wikipedia's inception), there used to exist

only driven information sources such as Britannica Encyclopaedia, where collaboration was never implemented. Today, Wikipedia stands way ahead in terms of content quantity as well as quantity.
- **Power Decentralisation**. Earlier, most of the services used to be administered and not automated. But Web 2.0 services follow a self-service model rather than being administrator dependent. For instance, Google AdSense is a self-service platform for Ad publishing. There is no administrator for allowing/rejecting the requests from the users. The users get to have a self-service system by Google which helps them deploy Ads on their site/blog quite easily.
- **Dynamic Content**. In a generation where blogosphere has overpowered the conventional mainstream media, Web 2.0 services have to be highly dynamic and proactive. If crowdsourcing is there then dynamicity follows by default.
- **SaaS**. With Cloud computing on a roll, more and more web services are taking the route of SaaS (Software as a Service). Software is available as a web service with no platform dependency at all.

2.2 WIKILEAKS

Although a lot of services based on Web 2.0 have been developed, from security point of view, particularly one has to be emphasized. In this chapter, we introduce Organization WikiLeaks which has gained international attention after posting classified documents and reports of governments, corporations and other high-profile organizations all over the world. WikiLeaks disclosed from security perspective sensitive diplomatic and military activities with an intention to make them transparent. The consequence was an increased gap between the citizens and states. WikiLeaks announcements were also a trigger for the "first cyber war" between organisation supporters and opponents, where also a part of critical infrastructure has been affected. There is no doubt; WikiLeaks caused tremendous changes in security sector as well in the role of a Western state and its citizen. Therefore, cyberspace security relevance in the time of Web 2.0 got an absolutely new dimension.

WikiLeaks is an international non-profit media organization which publishes news leaks based on their ethical, historical, diplomatic and political significance. Organization provides an innovative, secure and, most important, an anonymous way for sources to leak information to journalists, newspapers and to the general public (WikiLeaks, 2011). WikiLeaks operates, communicates and interacts with the outside world via the website known as Wikileaks.org. "Website that defines itself as a public service designed to protect whistle-blowers, journalists and activists who have sensitive materials to communicate to the public", came online on October 4, 2006 (Fogarty, 2010, p. 5). Since the website went online, it has posted an extensive catalogue of secret and classified material such as: e-mails from the University of East Anglia, in England – also known as 'Climategate', classified US military field reports from the War in Afghanistan – 'Afghan War Diaries', reports from War in Iraq – 'The Iraq War Logs' and U.S. State Department diplomatic cables – also known as "Cablegate" (Khatchadourian, 2010).

WikiLeaks: Complete Transparency?

The website WikiLeaks.org was originally created online in wiki[15] format, but gradually it has modified to a more traditional and restrictive publication model, so the documents cannot be edited by random readers (Steller, 2009). WikiLeaks describes itself as "an uncensorable system for untraceable mass document leaking and public analysis" (Khatchadourian, 2010). Documents and multimedia files can be leaked on a massive scale in a way which "combines the protection and anonymity of cutting-edge cryptographic information technologies" (WikiLeaks, 2011). According to Julian Assange and co-workers, they use their own coded software combined with OpenSSL[16], FreeNet[17], PGP[18] and Tor[19] as a main anonymity protection device (Leigh, 2011, pp. 52-53). According to Fenster, "WikiLeaks has established a powerful brand identity as a technologically sophisticated service capable of distributing data anonymously and publicizing its release." The success of the WikiLeaks has inspired also other supporters around the world and similar sites started to open, all patterned on the WikiLeaks model (Fenster, 2011, p. 7) (e.g., OpenLeaks.org, BrusselsLeaks.com, Transparency.AlJazeera.net).

WikiLeaks collects and publishes material that has been classified as confidential by corporations or government agencies. The idea of the organization is simple and clear: *complete transparency in politics and economy,* says Julian Assange (Kämmerling, 2011, p. 11). The website of WikiLeaks gives all the necessary information and directives to the potential informers how to hand over various documents or other materials.

---

[15] *The wiki concept was developed in 1995 as a collaboratively built site where content can be added or edited by any user. »It is web-based software that allows all viewers of a page to change the content by editing the page online in a browser. » (Ebersbach, 2008, p. 12). A wiki is a set of linked web pages where everyone has rights to edit everything, and editing is not discouraged but encouraged. Wikis are used to share general information with targeted audiences and to support collaborative work, such as projects or reports. In addition to text, wikis can feature text, graphics, video clips, and even plug-ins. Primarily due to the success of the free online encyclopaedia Wikipedia – The Free Encyclopaedia', wikis have become known to a wide audience (Ebersbach, 2008, pp. 13-14). Wiki is known as one of the key tools in Web 2.0.*

[16] *OpenSSL is an open source secure site connection system. It is a popular open source implementation of the SSL/TLS protocols. OpenSSL uses various cryptographic algorithms to ensure secure communication: symmetric key (secret key) encryption, asymmetric key (public key) encryption, message digests/digital signatures and certificates (http://www.openssl.org/).*

[17] *Freenet is free and open source software which operates as a location-independent distributed file system across many individual computers that allows files to be inserted, stored and requested anonymously (http://freenetproject.org/index.html).*

[18] *PGP – 'Pretty Good Privacy' is open source cryptographic system, to provide a secure communication in an insecure electronic environment (http://www.pgpi.org/).*

[19] *Tor - 'The Onion Router'is a sophisticated privacy tool that lets users navigate and send documents through the internet anonymously. It is a network of virtual tunnels that allows people and groups to improve their privacy and security on the internet. It was a US Naval Research Laboratory project, developed in 1995, which has been taken up by hacker around the world. It uses a network of about 2.000 volunteer global computer servers, through which any message can be routed, anonymously and untraceably, via other Tor computers, and eventually to a receiver outside the network. The key concept is that an outsider is never able to link the sender and receiver by examining »packets« of data (Leigh, 2011, p. 52-53).*

Anonymity as informant's top priority

There are four different ways in which an informant can hand over secret material to WikiLeaks:

a) *Via postal drops* (as an alternative method); digital copies on a data storage device or printouts sent to a P.O. Box in Australia by regular mail.
b) *In person;* the informant or intermediary hands over the document and video files to a WikiLeaks operator.
c) *Anonymous electronic drop box* (the preferred method of submitting any documents):
   – The informant uploads data through public internet access point (an internet café), the data is encrypted and transmitted to WikiLeaks (SSL encryption).
   – The informant uploads the data from his computer via the gateway network. This process involves cloaking the data's origin as well as providing counter-measures against bugging (SSL encryption).

After receiving the material, WikiLeaks operators remove any digital traces that would lead to the data's source and verify authenticity of the documents (they publish only original documents). The secret documents are fragmented into data packets distributed over numerous servers all over the world only to be reassembled on the reader's PC. WikiLeaks mirrors are accessible via hundreds of internet addresses. Redacted documents from WikiLeaks are first received by the publishers and journalists. Regular internet users can enter an operational WikiLeaks address and an upstream server, which does not store the data itself, but connects them to one or several other available servers (from WikiLeaks to the reader with SSL encryption). (WikiLeaks, 2011, Kämmerling, 2011, p. 12).

Breakthrough: Posting secret data

In January 2007, WikiLeaks announced 1.2 million documents waiting to be processed and published. A huge breakthrough and first major release was on April 5, 2010 when WikiLeaks released a classified US military video footage (entitled as "Collateral Murder") of a US Apache helicopter shooting into a crowd in Bagdad in 2007 which killed 12 people, including two Reuters journalists (http://www.collateralmurder.com/). The next release was on July 25, 2010, when WikiLeaks released more than 91,000 reports covering the war in Afghanistan from 2004 to 2010. Classified military reports called 'Afghan War Diaries', providing insights into unreported civilian deaths, secret operations against the Taliban, U.S. fears that Pakistan's intelligence service was aiding the Afghan insurgency, etc. On October 22, 2010, WikiLeaks released a package of 391,000 documents called 'The Iraq War Logs', with a focus on Iraq War between 2004 and 2009 (Zumwalt, 2010).

On November 28, 2010, WikiLeaks released approximately 250,000 documents, focusing on U.S. State Department diplomatic cables. According to BBC news "the diplomatic cables cover messages sent between 1966 and 2010 and originate from 274 US embassies, consulates and diplomatic missions." The entire archive of the

reports has been made available to five world-class news organizations: *The Guardian* (United Kingdom), *El País* (Spain), *Le Monde* (France), *Der Spiegel* (Germany) and *The New York Times* (United States) (BBC, 2010).

DDoS attacks

The response to the WikiLeaks US diplomatic cables release was dramatic and even more interesting. After the release of the documentation, WikiLeaks' website suffered disabling denial-of-service (DDoS[20]) attack. Cross-system attacks to servers tried to prevent the material from spreading throughout the internet. The hacker behind the attack appeared to be a patriot-hacker called "The Jester", describes himself as a "hacktivist for good" (Leigh, 2011, pp. 203-204). In response to the dissemination of classified documentation, the U.S. government began to exert pressure on organizations linked to WikiLeaks. The Amazon[21] which was hosting computer space to WikiLeaks and EveryDNS which provides free domain names dumped their client. A second type of systems that came under attack on a model parallel to the attack on technical infrastructure was payment systems. Shortly after the cables were published, several financial institutions, including *PostFinance*, *the Swiss postal system, PayPal*, *Bank of America, Visa and MasterCard*, closed Assange's and WikiLeaks' accounts[22]. None of these actions proved disabling. Hundreds of other servers around the world started hosting 'mirrors'[23] (copies of the site), the website was quickly up and running again using the Swiss domain named Wikileaks.ch. (The Economist, 2010). Some government departments and server providers have banned WikiLeaks in their countries, such as Australia, Switzerland (by a US service provider) and United States Military (Lennon, 2010).

After all 'government actions' against WikiLeaks, a group known as Anonymous launched DDoS attacks against websites operated by organizations opposing WikiLeaks. As a consequence of this attack Facebook and Twitter also closed the accounts and pages used by Anonymous (The Economist, 2010).

Anonymous strikes back

Online activists calling themselves Anonymous (AnonOps) have launched what is being called Operation: Payback. Operation: Payback had previously been directed against the websites of law firms that pursued online music pirates, as well as against the Recording Industry Association of America (RIAA) (Leigh, 2011, p. 207). Because of the WikiLeaks phenomena, today thousands of protesters and sympathizers

---

[20] *Distributed denial-of-service (DDoS) attack prevents a website or other network resources from being available to users (an attacker attempts to prevent legitimate users from accessing information or services) (http://www.us-cert.gov/cas/tips/ST04-015.html).*

[21] *'Amazon subsequently received a call from a staff member of the Homeland Security and Government Affairs Committee on the same day, who questioned the company about their relationship with WikiLeaks. Immediately after the call, Amazon decided to terminate their hosting duties to WikiLeaks' (Arthur, 2010).*

[22] *Wikileaks is a non-profit organization that depends on donations.*

[23] *WikiLeaks currently continues to operate with number of mirror sites (http://mirror.wikileaks.info/), if and when the main (www.wikileaks.org) site is down.*

around the world have joined a virtual internet gathering under Anonymous group. Anonymous also uses a typical web-attack strategy[24] - distributed denial-of-service (DDoS) and has targeted several websites: *Paypal, Mastercard, Visa, Amazon, the PostFinance site* and *the Swedish Prosecution Authority* (Walker, 2010). In the public statement, the Anonymous said: "ongoing attacks were a 'symbolic action' targeted at corporate website that had withdrawn services from WikiLeaks" (BBC, 2010). They also hit the websites of the politicians Sarah Palin and Senator Joe Lieberman, who are among WikiLeaks' loudest critics, and the Swedish prosecutor and lawyers involved in pressing for Julian Assange's extradition from London" (The Economist, 2010).

According to Hardy (2011, p. 157) Operation: Payback and the cyber-attacks launched by the Anonymous "were designed to intimidate governments and organisations into changing their policies on censorship, piracy and confidentiality issues."

AnonOps Communications: The New Strategy

Following a different agenda, today WikiLeaks is trying to spread the information from WikiLeaks' secret diplomatic cables and other leaked material in as many ways as possible. The new 'tactic' is called Crowdleak (previous project Operation: Leakspin) and the idea of the project is to release details from the leaked cables that the mainstream media had overlooked, summarise them "into chunks that everyone can understand" and post it in innocuous locations, as in YouTube videos, social networking websites and on message boards (BBC, 2010). In order to achieve this goal, they allow anyone to volunteer to help them by writing and translating articles, fact checking, editing articles and finally making sure the website remains active and popular (Crowdleaks, 2011).

Based on the facts and information, as well as previous and current events linked to WikiLeaks we can agree with Micah Sifry saying *"age of transparency is here. Not because one transnational online network dedicated to open information and whistle-blowing named WikiLeaks exists, but because the knowledge of how to build and maintain such networks is now widespread. WikiLeaks is just one piece of a much larger continuum of changes in how the people and the powerful relate to each other in this new time changes that are fundamentally healthy for the growth and strength of an open society. Secrecy and the hoarding of information are ending; openness and the sharing of information are coming."* (*http://www.huffingtonpost.com/micah-sifry/wikileaks-assange-micah-sifry_b_820671.html, 6 June 2011).*

[24] *In January 2011, after Anonymous being accused of hacking many websites, they explained in the open letter to the UK government, what is the difference between a DDoS attack and hacking: »hacking as such is defined by the law as 'unauthorised access to a computer or network', whereas a DDoS attack is simply a case of thousands of people making legitimate connections to a publicly accessible webserver at the same time, using up the entire bandwidth or processing power of the given server at once and thereby causing a huge 'traffic jam'.«*

Conclusion

Throughout the 40 years of existence and expansion of ICT, security relevance of cyberspace has changed dramatically, both, nationally and globally, just as the societies have. Certainly, one of the decisive factors causing this was the commercialisation of the information technology and its expansion beyond the national security system. This has also been proved by an analysis of basic concepts which saw cyberspace, both, as a threat and a comparable advantage. At first, they were derived from a defence and military area and saw ICT mainly as a technology which will alter the perception of reality (from the point of view of intelligence), increase the preciseness of conventional weapons beyond imagination as well as establish a decentralised command and control system which will function even in the most impossible of situations. The more the number of civilians increased, the more the concepts were emphasising the part of information warfare, which is to be based on similar grounds as publicity and psychological operations. In light of global geostrategic changes, the 1990s represented the peak of ideas on information warfare, the more radical ones even presuming the conflicts to completely move from a realistic space into a virtual one. Of course, this has not happened. What is more, state structures acquired a completely equal "co-speaker" within cyberspace, both, in form of technically competent individuals and international associations. The aim of the present paper was to focus especially on the latter ones. Although it has been assumed for a long time that, especially in the field of politics and security, there was a strict separation line between the developments in the cyberspace and those in reality, this line was slowly crossed by expanding the services based on the second-generation web. At first, the users, of course, had to be motivated to convert from passive readers into active ones, who would also produce such information. In the first phase, the services, such as YouTube, Wiki, file exchange and sharing portals and, last but not least, social networks, thus had to satisfy the users' need for entertainment, before becoming the backbone of global communication. From a state's point of view, the ghost has left the bottle, intentionally or not. Today, it is therefore impossible to maintain a high level of confidentiality and privacy, which is, all in all, also proven by different Slovenian examples ranging from Udba.net to the Mikstone1 blog. The tendencies for perfect transparency (which surprisingly stopped at publishing information on the functioning of authorities in western countries) have undoubtedly culminated in the WikiLeaks movement with its publishing, but mainly accumulation of data and their decentralised storing. This aspect is important mainly from a political and morally ethical point of view, while, from a security point of view, lateral developments may appear even more important. Cyber battles between the supporters and opponents of the project have also affected parts of critical infrastructure. Of course, in the end, we should mention the responses which have been rather radical, particularly at state levels. In the USA, even students have been warned that browsing through and spreading WikiLeaks data may affect their chances of employment in the national security sector. Numerous ideas have emerged on how to put norms on cyberspace and operations within it, both, at national level as well as internationally (UN). It is an undisputable fact that dealing with cyberspace from a security point of view no longer implies warning against potential future misuse, because it has already become a reality. Centres of social power have changed accordingly,

the most important ones including the platforms and services called Web 2.0. While, throughout human history, physical communication has been subjected to geostrategic efforts, the 21st century made a decisive emphasis on the control of digital communications, both physically and with regard to services. Commercial actors and certain individuals as well as nation states and international organisations dealing with collective defence and security are all well aware of this fact. There is only one question arising thereof – will we enter a new Cold War, which could also take place in the relation state-citizen or in the fight against everybody within cyberspace, or such use of ICT will prevail, which will reinforce positive peace, dialogue, cooperation and solidarity.

Bibliography

1. *Arquilla, J., Ronfeldt, D.,1999. The Advent of Netwar: Analytic Background. Studies in Conflict and Terrorism 22 (3), pp. 193-206.*
2. *Arthur, Charles, 2010. WikiLeaks under attack: the definitive timeline. http://www.guardian.co.uk/media/2010/dec/07/wikileaks-under-attack-definitive-timeline, 1 June 2011.*
3. *BBC, 2010. US embassy cables: The background. http://www.bbc.co.uk/news/world-us-canada-11862320, 4 June 2011.*
4. *BBC, 2010. UK Government websites may be next pro-Wikileaks focus. http://www.bbc.co.uk/news/technology-11990288, 3 June 2011.*
5. *Bilgin, P., 2003. Individual and Societal Dimensions of Security. International Studies Review 5 (2), pp. 203-222.*
6. *CASAGRAS, an EU Framework 7 Project, 2009. http://www.rfidglobal.eu/userfiles/documents/CASAGRAS26022009.pdf, 2 June 2011. .*
7. *Chertoff, M., 2008. The cyber security challenge. Regulation & Governance (2008) 2, pp. 480-484.*
8. *Crowdleaks, 2011. Official website: http://crowdleaks.org/, 4 June 2001.*
9. *Davies, J. G., 2011. From Crowdsourcing to Crowdservicing. Internet Computing 15(3), pp. 92-94.*
10. *Deibert R. J. in Rohozinski R., 2010a. Risking Security: Policies and Paradoxes of Cyberspace Security. International Political Sociology 2010 (4), pp. 15-32.*
11. *Deibert R. J. in Rohozinski R., 2010b. Liberation vs. Control in Cyberspace. Journal of Democracy 21(4), pp. 43-57.*
12. *Denning, D. E.,1999. Information Warfare and Security. Indianapolis: Addison-Wesley.*
13. *Der Derian, J., 2000. Virtuous war/virtual theory. International Affairs 76(4), pp. 771-778.*
14. *Ebersbach, Anja, Glaser Markus, Heigl Richard, Warta Alexander, 2008. Wiki: Web Collaboration: Berlin, Heidelberg: Springer.*
15. *Evropski ekonomsko-socialni odbor: TEN/436 Nova" uredba o Evropski agenciji za varnost omrežij in informacij. Mnenje Evropskega ekonomsko-socialnega odbora o predlogu uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA), 2011.*
16. *Fenster, Mark, 2011. Disclosure's Effects: WikiLeaks and Transparency. Florida: Levin College of Law.*
17. *Fogarty, Jim, 2010. Wikileaks, transparency, and national security: A website that exposes secrets has raised the ire if the U.S. government. New York: The Epoch Times, p. 5. http://epoch-archive.com/a1/en/ca/yeg/2010/06-Jun/17/Page%2005%20World.pdf, 31 May 2011.*

18. *Geers, K.,2009. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective 18, pp. 1-7.*
19. *Geers, K.,2010 (a). The challenge of cyber attack deterrence. Computer law & security review 26 (2010), pp. 298-303.*
20. *Geers, K.,2010 (b). Cyber Weapons Convention. Computer law & security review 26 (2010), pp. 547-551.*
21. *Hardy, Keiran, 2011. WWWMDs: Cyber-attacks against infrastructure in domestic anti-terror laws. Computer Law & Security Review. 27-2, pp. 152-161.*
22. *Harknett R. J. in Stever J. A., 2011. The New Policy World of Cybersecurity. Public Administration Review • May | June 2011, pp. 455-460.*
23. *http://arpanet.co.tv/, 20 May 2011.*
24. *http://www.huffingtonpost.com/micah-sifry/wikileaks-assange-micah-sifry_b_820671.html, 6 June 2011.*
25. *http://www.jgzumwalt.com/index.php/articles/251-assessing-wikileaks-damage-to-us-national-security, 30 May 2011.*
26. *http://www.techpluto.com/web-20-services/, 28 May 2011.*
27. *http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317, 25 May 2011.*
28. *Hughes. R., 2010. A treaty for cyberspace. International Affairs 86: 2 (2010), pp. 523-541.*
29. *In the Crossfire Critical Infrastructure in the Age of Cyber War, 2009. http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf, 2 June 2011.*
30. *Kämmerling, Andi, 2011. What is behind Wikileaks? Domo Ringier AG, Corporate Communications, March 2011, p. 10-13. http://domo.ringier.com/wp-content/uploads/2011/03/DOMO_2011m03_en1. pdf, 31 May 2011.*
31. *Khatchadourian, Raffi, 2010. No Secrets: Julian Assange's mission for total transparency. The New Yorker: http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian, 1 June 2011.*
32. *Klimburg, A., 2011. Mobilising Cyber Power. Survival 53(1), pp. 41-60.*
33. *Kling, R., 2000. Learning About Information Technologies and Social Change: The Contribution of Social Informatics. The Information Society 16(3), pp. 217-232.*
34. *Leight, David and Harding Luke, 2011. WikiLeaks: Inside Julian Assange's War on Secrecy. London: Guardian Books.*
35. *Liotta, P. H., 2002. Boomerang Effect: The Convergence of National and Human Security. Security Dialogue (33) 4, pp. 473-488.*
36. *Malešič, M., 2004. Environmental security; a case of Slovenia. In: Mahutova, Katarina - Barich, John J., Kreiznebeck, Ronald A. (eds.). Defense and the environment: effective scientific communication, (NATO science series. Series IV, Earth and environmental sciences, vol. 39). Dordrecht; Boston; London: Kluwer Academic Publishers, pp. 139-152.*
37. *Michael, J. B., Tikk, E., Wahlgren, P., Wingfield, T. C. (2010). From Chaos to Collective Defense. Computer 43 (8), pp. 91-94.*
38. *Munro, I., 2009. Defending the Network Organization: An Analysis of Information Warfare with Reference to Heidegger. http://org.sagepub.com/content/17/2/199.*
39. *Myrli, S., 2011. NATO and Cyber Defence. Military Technology 2011(3), pp. 86-90.*
40. *Nissenbaum, H., 2005. Where computer security meets national security. Ethics and Information Technology (2005) 7, pp. 61-73.*
41. *Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1), p. 3677. Uradni list RS, št. 27/2010 z dne 2. 4. 2010.*

42. *Saydiari S., 2004. Cyber defense: art to science. Communications of the ACM 47 (3), pp. 53-57.*
43. *Steller, C., 2009. What is Wikileaks? http://minnesotaindependent.com/28719/what-is-wikileaks, 2 June 2011.*
44. *Sund, C., 2007. Towards an international road-map for cybersecurity, Online Information Review 31(5), pp. 566-582.*
45. *Svete, U., 2005. Varnost v informacijski družbi. Ljubljana: Fakulteta za družbene vede.*
46. *Škrubej, J., 2008. Hladna vojna in bitka za informacijsko tehnologijo. Ljubljana: Pasadena.*
47. *The Economist, 2010. The 24-hour Athenian democracy. http://www.economist.com/blogs/babbage/2010/12/more_wikileaks, 3 June 2011.*
48. *The Economist, 2010. The war on WikiLeaks: Sound, fury but few results so far as America tries to fight back against WikiLeaks. http://www.economist.com/node/17674107, 2 June 2011.*
49. *US Pentagon to treat cyber-attacks as ‚acts of war', 2011. http://www.bbc.co.uk/news/world-us-canada-13614125, 2 June 2011.*
50. *W32.Stuxnet Dossier, 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2 June 2011.*
51. *Walker, R. Chrisopher, 2010. A brief history of Operation Payback. http://www.salon.com/news/feature/2010/12/09/0, 3 June 2011.*
52. *Walt, S. M.,1998. One world, many theories. Foreign Policy (Spring 1998), pp. 29-35.*
53. *Waltz, K. N., 2000. Structural Realism after the Cold War. International Security 25 (1), pp. 5-41.*
54. *WikiLeaks, 2011. Official website: www.wikileaks.org, 30 May 2011.*
55. *Zumwalt G., James, 2010: Assessing WikiLeak's Damage To U.S. National Security. Human Events, p. 12.*

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.3

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.*

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.4

Maja Bolle

Strokovni članek

INFORMACIJSKA VARNOST IN ODPRTOKODNA PROGRAMSKA OPREMA

INFORMATION SECURITY AND OPEN SOURCE SOFTWARE

Professional article

Povzetek Informacijska varnost je ob vedno večji odvisnosti od računalniških sistemov pomembna tema tudi za javno upravo. Ob vedno večjem številu napadov in drugih posegov v integriteto operacijskih sistemov in drugega programja so se mnoge države odločile za prehod na odprtokodno programsko opremo, ki poleg varčevanja pri nakupu programskih licenc državam omogoča tudi večji nadzor nad to opremo. Nekatere raziskave govorijo v prid varnosti zaprtokodnih sistemov, spet druge priporočajo uporabo odprtokodnih. Podatki kažejo, da ima odprtokodna programska oprema na marsikaterem področju boljše varnostne mehanizme kot zaprtokodna, vendar pa ima tudi ta svoje omejitve. Zaradi teh mora biti prehod držav na odprtokodno programsko opremo dobro premišljen.

Ključne besede ***Odprta koda, odprtokodna programska oprema, zaprtokodna programska oprema, informacijska varnost.***

Abstract In times of increasing dependence on computer systems, information security emerges as an important issue for public administrations. Many governments have made a transition to open source software; the reason being not just financial, but connected to increasing numbers of operating systems security issues. Having more control over the systems is also key. Some researchers speak in favour of proprietary software, others in favour of open source software. Data shows, however, that open source software leads over proprietary software in security mechanisms, although it is not without its limitations. This is the reason that states transitioning to open source software must take precautions in doing so.

Key words ***Open source, open source software, proprietary software, information security.***

Introduction

We live at a time in which life and work is no longer possible without a computer. It is therefore essential to address the question of information security. Due to increasing interventions into the integrity of the most utilized operating systems and other software, numerous countries have decided to transit to open source software. Some countries, such as Slovenia, are still searching their way through the transition. Although most countries have transferred to open source software for economic reasons, security reasons should not be disregarded (Kimberly, 2005).

Open source software is a term used for describing software in which the source code is freely accessible and which can be used free-of charge. The operation of such software can be investigated and its original, supplemented and modified copies can be changed. The above is not possible to do with proprietary software. The terms of its use are written in various licenses that include guidance on the use of the Open Source Initiative. The most important criteria are free distribution, access to the source code and permission to modify and integrate the source (http://www.opensource.org/).

1 OPEN SOURCE HISTORY AND PHILOSOPHY

The beginnings of open source software date back to the 1950s. The first computers were large and, considering contemporary standards, not very capable. They also had very poor software. User interfaces were unfriendly and software capabilities were lower than what the hardware enabled. At that time, programmers were hard to find. Consequently users started to unite with the intent to exchange ideas and software that would make better use of the hardware capabilities and satisfy their needs. Thus the first associations uniting such enthusiasts were formed – the most well known association is the SHARE association, founded in 1955. However, at the end of the 1960s the system changed. The companies that were selling hardware also enclosed software which, at the time, was free of charge (http://tinyurl.com/6jgg3ut). Hence, the market offering software for payment was getting stronger every day.

1.1 Origin of the first open source software

1.1.1 Unix

In 1969, Ken Thompson produced an operating system UNICS (Uniplexed information and computing services) that was later renamed Unix. The AT&T company, at which Thompson was employed, had seen a business opportunity in Unix and requested its licensing. The first licence was free of charge and provided considerable freedom to users. However, the AT&T company did not offer support for this licence. All software is inevitably confronted with the so-called bug phenomena, which are faults in the programme code resulting in undesired and unexpected outcomes on use. All this had a direct influence on Unix users who had started to unify into groups, collectively eliminate bugs and to improve Unix – something that the AT&T company did not foresee with its license. However, the source was closed in such a way that the groups had to pay AT&T to access the source code.

This was also done by the BTL research group that copied the source code in the C Programming Language. By making modifications to the code it made it possible for Unix to operate on any hardware and on any computer. It was also made possible for the users to produce their own drivers for equipment they needed at work (Weber, 2004).

1.1.2 BSD

The University of California, Berkeley, at which Unix was used, played an important role in the development and modification of open source software. Researchers, Bill Joy and Chuck Haley, developed and supplemented Unix's core. In 1978, Joy produced a number of add-ins for Unix that, together with the core, formed a package named Berkeley Software Distribution (BSD). BSD was not an independent operating system, but a Unix distribution. BSD became extremely popular among students and researchers and Unix was quickly abandoned in favour of it (Weber, 2004).

In 1968, the predecessor of today's internet, ARPANET, started to operate. At first it provided connection between the American Department of Defence's agency DARPA (Defense Advanced Research Projects Agency) and other research institutions.

DARPA's aim was to communicate with other institutions via ARPNET. This, however, was made difficult due to the incompatibility of different computers and operating systems. DARPA therefore asked the BSD researchers to develop software that would work on all hardware equipment; version 4.2.

The BSD programme from 1983 included a new protocol called TCP/IP used for internet communication that is still used and serves as the base of today's internet. The internet and the TCP/IP protocol are the main reasons why BSD became widely distributed over the internet.

In the meantime, AT&T tightened the Unix license conditions thus increasing its price. In 1989, the price of the license was 250,000 USD. Since the universities could no longer afford to buy Unix, they started using BSD (Weber, 2004).

1.1.3 Free software foundation

Richard Stallman is a founder of the Free Software Foundation. The aim of this non-profit making institution was to create a free of charge operating system - the source code of which would be available to everyone and could be freely changed. The operating system was named GNU. In 1984, he wrote the GNU Manifest in which he explained the meaning of the term free software.

The term does not necessarily refer to a free of charge software, but only to free software: In this sense free refers to the accessibility of the source code and the possibility to modify it (Wynants, 2005). This means that Stallman is not opposed to software

having a price with which the programmer's work is paid, but wants to keep it free in its essence (Spanish libre). The manifesto contains four principles that still apply:

1) freedom to use the programme for any kind of purpose (freedom no. 1);
2) freedom to study the programme and modify it as desired. Requirement to access the source code (freedom no. 1);
3) free distribution of copies (freedom no. 2);
4) freedom to improve the programme and publish improvements (and adapted versions) to the benefit of the community (freedom no. 3); precondition for which is access to the source code.

Since Stallman was aware that these basic freedoms could be taken advantage of, he has additionally improved the license. Such a license is the opposite of copyright and is called a General Public Licence (GPL). The software licensed under GPL can never become proprietary. This applies also to the modified programme equipment that derives from free software. Only a combination of proprietary and free software can be issued and even that only under the condition that everything is licensed under GPL (Weber, 2004). The GPL license was supplemented throughout time (the last version is GPL v3) and used to serve as a basis for more specific licenses (http://tinyurl.com/hdpo9).

1.1.4 Linux

Linux is the world's most widespread open source operating system in the field of supercomputers and servers. It owns 91 percent of the market share among supercomputers, followed by Unix with three percent and Windows with one percent (http://tinyurl.com/27l5wvh). Linux also owns the largest market share among servers, which is as much as 70.71 percent (http://tinyurl.com/3hdqvgd). However, Linux still has the lowest share in desktop computers (5.1 percent), while Windows owns 85 percent and Mac OS X 8.3 percent of the market share (*http://tinyurl.com/28lpgq*).

Linux was created in 1991 under the management of the then 21 year old Linus Torvalds. On 25 August 1991, in a discussion group called comp.os.minix, he declared his intention to develop a kernel for a new operating system. On 17 September, he published his first version of the Linux operating system kernel on the internet. He invited people to test his system and improve it. Since Linux was able to obtain more and more supporters and developers every day, the first version 1.0.0 was published in 1994 (Weber, 2004). Nowadays, Linux can operate on almost any computer structure (desktop computers, supercomputers, servers, wrist watches, Playstation 3 game console) (http://www.Linuxfordevices.com/).

Since Linux is nothing more than a core of the operational system, developers from all across the world developed graphical interfaces, desktops, programmes, drivers etc. for it and combined everything into a package called distribution. The distributions are based on an individual kernel of the operating system (e.g. Linux, BSD) and differ from one another according to what type of operating system, desktop and

repositories they include. The most widespread and popular distribution of Linux is Ubuntu that over 12 million people use on their desktop computers (Jose, 2011).

2 SECURITY OF OPEN SOURCE SOFTWARE

Which system is more secure: the one with less kernels or a system which can quickly make corrections or perhaps a third one, the vulnerability of which can affect less people. There are a lot of researchers that are in favour of one or the other; most of them focus only on one of the mentioned aspects (Laurie, 2006). This paper is striving to present the issue in the broadest context possible and in different areas that are connected to information security in one way or another.

2.1 Large number of distributions

According to the Distro Watch data (http://distrowatch.com/), there are currently 320 distributions in the world all based on operating systems similar to Linux and Unix. The actual number of distributions is in fact much bigger, as anyone can make their own distribution at home. Due to a large number of distributions the possibility of malware [1] software being written for a specific distribution is much smaller than with proprietary software. In reference to two of the most widespread proprietary operating systems we are not even familiar with the term distribution, for every individual purchases an operating system that no longer has the form of distributions, but only versions (Apple and its Mac OS X with versions Snow Leopard, Lion and Microsoft's Windows with versions Windows XP, Vista, 7...). Each version of these proprietary operating systems is based on a different kernel, which reduces the transferability of malware among them. However, the malware written for proprietary systems has a much larger distribution value due to a small number of versions and the mono-culturality of Microsoft's operating systems. This is because these versions are modified less frequently than those for the open source operating systems. In addition, the probability of malware infecting a large number of distributions is less likely to occur due to differences in code. From the aspect of information security, a large number of distributions, which is characteristic of open source software, is therefore considered to be an advantage.

2.2 Malware

Malware is written for a specific operating system and its version, as the source code differs, is different for each version. To this day we have witnessed over two million cases of malware for the Windows operating system, 1989 cases of malware for the Linux operating system and 48 cases for the Apple Mac OS X (Kalkuhl, 2009). The number of malware cases has considerably increased during the last two years – both in open source and proprietary operating systems. The recent reports by the Kaspersky institute state that the reason for the increase in the number of malware cases lies in the fact that both operating systems are becoming more popular (http://

[1] *Malware software is software that wishes to be infiltrated into a computer system and damage it without the user consenting to such an action (Meintjes, 2011).*

tinyurl.com/44x9pxd). The report also states that Linux is the most affected operating system that resembles Unix. It is also the most widespread. Nonetheless, the statistics demonstrate that Linux was attacked mainly through servers and less through the desktop area (Sapronov, 2007; Germain, 2008).

Despite the fact that up to this day we have witnessed as many as 1989 cases of malware for open source software its lifespan is very short and it does not cause as much damage to Linux as to the Windows operating system. The reason for this lies in the administrator's access (superuser account – more widely known as ROOT) which is, for safety reasons, automatically deactivated in Linux, BSD and other Unix-like operating systems to prevent users that are unskilled in using the operating system from damaging it (http://tinyurl.com/o4foa). In practice this means that we set a password that enables us to modify all settings in the operating system. It is different with the Windows operating systems that had not known an actual blockade of administrator access with a password up until the versions Vista and 7. Nonetheless, this blockade is still not very severe as the users can modify a number of things without having administrator access. (Schneier, 2006). The Apple's operating system Mac OS X is based on Unix's kernel in which the administrator's access is disabled by default and requires the user to type in the password, which is a positive trait.

(http://support.apple.com/kb/ht1528). If an infection with malware occurs in Linux the damage will not be significant, since this equipment will not have administrator access for the entire system. Its effect will therefore be either local or there will be no effect at all (http://librenix.com/?inode=21; Koetzle, 2004). Similar findings were stated in the research Analysis of the Impact of Open Source Software from 2001 (http://tinyurl.com/6lyeod8) in which the impact of viruses on various operating systems was studied: At the time, Windows had over 60,000 viruses, while Mac OS X and Linux both had 40 respectively. Despite the fact that most viruses written for Windows did not cause great damage, some hundreds of viruses were much more harmful. Two thirds of all known viruses have caused considerable damage to the Apple's Mac OS X system, while not even one of the Linux viruses caused great damage or spread more widely across the system (Peeling, 2001). The safety of operating systems similar to Unix can be considerably threatened by the so-called rootkit that enables covert access to a computer system and the use of administrator privileges (Chuvakin, 2003).

As we can see, the amount of existing malware for a specific operating system is not that important. What is more important is the impact malware can have on a system in terms of level and scale.

2.3 Do many eyes really see more?

The many eyes system is a system of inspection, with which every user can have an overview of the source code of the open code software – in theory this minimizes

the possibility for open code software to contain a malicious code such as backdoor through which an unauthorized person could obtain access to the system.

The defenders of open source software often argue that the many eyes system enables a rapid detection of bugs in the code. However, this is not always the case in practice. Nowadays most users are not skilled in programming, cannot read the source code or recognize deficiencies or possible backdoors in them. Open source software is used for everyday chores, such as writing texts, management of tables and writing e-mails. Nonetheless it still provides insight for those who are interested in it and capable of it. This is an important difference, for proprietary systems do not enable such insight (Laurie, 2006).

There have been a number of cases in history when vulnerabilities were not discovered for several years even though the open source software was examined by a number of people. One of the most interesting cases is Ken Thompson's backdoor. He was a developer of the Unix system into which he incorporated a backdoor. Thompson revealed this only after fourteen years. With this experiment Thompson wanted to demonstrate that we should not rely on other people too much. He is convinced that only the code we write ourselves is safe (O'Dowd, 2004). At this point we should address the question of the human factor. Even though the code was examined by a number of people it does not mean that the examination was detailed enough or that the examiners were competent enough to detect all vulnerabilities.

2.4 Time for correction

Time for correction is a time between the moment in which the vulnerability in the code has been detected and the time at which the correction has been made. This time has to be as short as possible – the longer the vulnerability is left without a correction, the more endangered is the system's security. Research comparing the security of Windows operating systems and different Linux distributions (Debian, Red Hat, Mandark) conducted over one year has demonstrated a number of threats, the time necessary for the production of the correction and a number of corrected threats (Koetzle, 2004). On average Windows spent the least amount of time, that is 25 days on the production of corrections. It is followed by Linux's distributions Red Hat and Debian with 57 days and Mandark with 82 days.

However, this data alone does not suffice to make a comparison of the operating systems: It was discovered that the Windows operating system has the highest level of threats (67 percent of all threats), followed by Red hat with 56 percent of the same level threats. The research has also included the measuring of time that the providers require for insertion of corrections into the distribution. For the Windows operating system this time was the same as for the production of corrections, since the distributions of the Windows systems do not exist. On average the Debian would require only 32 days, which is a lot less than the time required for the production of corrections (57 days). The same applied for Red Hat with 47 days. Debian was so fast

because this was the only examined distribution that was being used without a new installation of the entire system being required (rolling release).

The time of production of these corrections is not the only important security element. The most important are the users, because they have to install the corrections. Microsoft users have been threatened by nine vulnerabilities of the highest level. Nonetheless, most examined users have not installed the corrections for over 305 days. This means that on average, they have been at threat for 305 days despite the fact that Microsoft produced the corrections after approximately 25 days (Koetzle, 2004).

If people discover vulnerabilities in the open source software through the system many eyes they immediately publish the news on internet pages, forums etc. (such as Ubuntu Bugs Launchpad – https://bugs.launchpad.net/ubuntu/). The developers of open source software eliminate weaknesses in the shortest time possible. However, there exist differences among the developers of various open source software. On average the Apache issues corrections on a daily basis, which means that a certain vulnerability seldomly exists more than a day. Ubuntu, the most widespread Linux distribution, issues corrections in reference to priority order determined through the Ubuntu Bug Launchpad.

The providers do not refresh their bases in accordance with the everyday open source software. This deficiency is eliminated by the repository that enables the users to install the latest version of the programme independent of the providers of the distribution and in the moment the developer publishes it. The repository was made for purposes of faster distribution of the newest version of software equipment to users and in order for the developers to obtain faster feedback about the quality of the equipment, which speeds up its development (Laurie, 2006). In 2007, the Ubuntu issued the **Personal Package Archive** (PPA) software with the purpose to additionally expedite and facilitate the distribution of software through repositories (Humbrey, 2011). However, not all repositories are safe and it is therefore recommendable to use only those repositories that are verified and in no way "suspicious".

The proprietary operating systems Windows and Mac OS do not have the many eyes system, therefore security is provided by the developers of each system individually. They do not publish all vulnerabilities, for which reason we are unaware of how long we are exposed to them or their actual number.

As we can see, a large number of published threats does not mean that the system is more vulnerable, but more transparent. Since we cannot see all vulnerabilities in proprietary software because of its intransparency, the open source software is an advantage.

2.5 Security through transparency or concealment

We have heard many times that hiding of the source code provides better security, however in practice this is not the case. One of the first cryptologists, Auguste Kerckhoffs, wrote six principles of good cartography in 1883. These principles are nowadays known as the Kerckhoffs' Pinciple, which states that a good coding system is safe even if we know everything except the encryption key about it. Kerckhoffs also rejects the principle that it is possible to provide security only by means of concealment. He does not demand that the encoding system is public, but stresses that secrecy does not ensure greater security; on the contrary, it can even threaten it (Kovačič, 2006). A covert system can threaten the security by containing faults that could be, if such a system was public, detected and repaired. Bruce Schneier, an expert on information security and a cryptologist says: "I cannot remember any cryptographic system developed secretly, in which, after being introduced to the public, the cryptographic community would not find a mistake." (Schneier, 2002).

Something similar occurred in the famous database case of the Borland InterBase, in which a backdoor was discovered in 2000. That was the year in which the company published the software source code that prior to this occasion had been proprietary or closed.

The programmers discovered that in 1994 a backdoor had been intentionally added to the database. The door enabled an individual to have full access to all information and even to insert information and contents with the user name "politically" and the password "correct". It is even more alarming that the database was used by the Boston stock market and large corporations such as Motorola, Nokia and Boeing. The programmers of open source software made rapid corrections that closed the backdoor (Poulsen, 2001).

In the spirit of open source today, even Microsoft provides countries with access to the source code; however, it does so only under conditions laid down in the Government Security Programme contract. The contract was signed by approximately 60 countries, including NATO states, China and the Russian secret service FSB (Espiner, 2010). Nonetheless, Microsoft is the one that decides if the source code will be revealed to a specific country or not. The countries to which Microsoft does not enable access to the source code are: Venezuela, Cuba and other countries whose public administrations transferred to the open code software. Richard Clayton from Cambridge University draws attention to the weaknesses of such a system: the countries can detect vulnerabilities in security much more easily and thus use them to attack other states, for they do not publish the information about the mentioned vulnerabilities. The latter are known only inside the system which has access to the source code. Another limitation of the Government Security Program is that it provides countries with an insight into the source code, but does not enable its modification (http://tinyurl.com/3fldnhr).

3 TRANSFER OF NATIONAL PUBLIC ADMINISTRATIONS TO OPEN SOURCE SOFTWARE

Recently, more states decided to transfer to open source software. Some of them are making only a partial transfer (e.g. in certain government agencies) and use only open source software (these are the USA, France, Germany, the Czech Republic, Macedonia, South Africa, the Philippines). Other countries have decided to make a full transfer to open source software (China, Russia, Brazil, Venezuela, Pakistan, Cuba, Turkey, Malaysia and Spain) meaning that they use the distributions of the Linux or BSD operating systems together with the relevant software. Most countries that have decided to do a full transfer have created their own national distributions of the operating systems that contain specific software (the one that is used in a specific public administration). In order to ensure better security these countries made their own repositories, which are updated by their public institutions. The software found in these repositories was developed specifically for the needs of state institutions. This contributes to greater security of the operating systems, since the software located in repositories is examined and developed by the states themselves. In addition to a reduction in costs, security is one of the main reasons why national public administrations decided to transfer to the open source software (Lewis, 2006). In 1999, when the first reports that the American National Security Agency (NSA) had entered a backdoor into every copy of the Windows 95 operating system (Campbell, 1999), states have started to question the security of and the control over the operating systems of the Microsoft company. They were concerned also because of Microsoft's mono-cultural tendencies, for the company owns over 80 percent of the desktop computers market share. In addition, Microsoft had started to supplement the code in such a way that it limited its operation on other systems thus "chaining" the states to it (vendor-lock in). This has encouraged countries to think about alternative programme solutions that would provide better control over computer systems, greater transparency, greater independence from Microsoft and a possibility to develop and adjust the system to their needs (Geer, 2003). Numerous countries have seen the solution to their problems in open source software.

A few examples: In Venezuela an independent operating system was developed. This system, based on the Debian Linux distribution, is called Canaima. National decree no. 3390 (http://tinyurl.com/3pdksvv) prescribes the use of Canaima in public administration and further states that all software specifically developed for public administration would have to be licensed under GPL (Cleto, 2004). For Hugo Chavez one of the reasons to transfer to open source software (in addition to security and the desire to be independent from the USA and Microsoft) was the information that 75 percent of licensed software is distributed to other countries, 20 percent for the support of foreign agencies, while only five percent is left for the Venezuelan programmers (Proffitt, 2002). Russia as well has decided to transfer to open source software. However, its transfer is still in progress and will be completed in 2012 or at latest by 2015. According to Putin, one of the main reasons for the transfer was the desire to be less dependant on other countries in the use of proprietary software (Morozov, 2011).

By 1990, China had also demonstrated interest in open source software. In 2005 it produced the first version of its national operating system of Linux distribution, Red Flag Linux that is used in the public administration. At the same time China has developed an Asianux distribution that was oriented towards Asian markets, for it supports Chinese characters (Blanchard, 2007). China, whose economy is growing extensively and with which also grows the requirements for a more localized software that satisfies the needs of local companies, is becoming more competitive in world markets through the development of its own software (Saxenian, 2003). Once, China had one of the highest levels of piracy in the world. This number has started to reduce due to the use of open source software. In this way China can provide greater information security and independence (Lock, 2006).

One of the largest supporters of open source software is the European Union. Some of the largest open source projects and solutions have originated within this organization (Gonzalez-Barahona, 2006). There has been an Open Source Observatory and Repository for European public administrations (OSOR) established in the European Union. The purpose of this institution is to develop special applications and the open source software to be used in the public administration within the EU. By means of this project the EU desires to reduce the costs in the public administration and standardize the formats and procedures across the union, reduce the expenses of e-government and help spread good practices (http://www.osor.eu/about).

The situation on the use of open source software in the public administration in Slovenia will be presented in a brief overview: In 2003, Slovenia adopted a document, The Policy of the Government of the Republic of Slovenia in the development, deployment and application of software and the solutions based on open source (Politika Vlade RS pri razvijanju, uvajanju in uporabi programske opreme in rešitev, temelječih na odprti kodi). Among other things the document states that the country will support the use of open source solutions and treat them equally together with the licensed solutions and support education on how to use them (*http://tinyurl.com/6gyjnou).* At the moment the document has not yet been put into practice. So far, based on a research Assessment of economic justification of the MS EA for the period between 2003 and 2005 (Ocena ekonomske upravičenosti MS EA za obdobje 2003-2005) (*http://tinyurl.com/68u2cm7)* in which it was established that the use of license software is more wise from a financial aspect than the use of the open source software, the state has been purchasing MS Office licensed equipment for public administration through public tenders. However, there are some bright exceptions in the public administration, such as the Supreme Court of the RS that completed the transfer between the years 2006 and 2007, thus changing the MS Office package with the Open Office package, the Microsoft Internet Explorer browser with the Mozilla Firefox and installing an open source application for e-mails called Thunderbird on 4600 work posts. The Supreme Court has established that this decision helps them save approximately 400,000 € per year (http://tinyurl.com/6hszcy5).

The year 2011 was a sort of a turning point in this domain for Slovenia, for the country published a study about its intention to gradually transfer to the use of open source software by 2015; at first merely by replacing the MS Office systems with the Open Office systems and in time by replacing all operating systems with the open source systems such as Linux distributions (*http://tinyurl.com/3f69g8u*). The mentioned study has initiated a number of critiques, mainly from the providers of licensed programme solutions. The Microsoft company has declared that with such a decision the Government would cause them to loose at least 2.5 million Euros per year (Mihajlovič, 2011).

In terms of open source software application Slovenia is behind in comparison to other EU member states. At this point we should nonetheless draw attention to a possible problem in the transfer of Slovenia's public administration to open source software. The problem lies in the applications that were made especially for the public administration – they are made solely for the Microsoft environment. Other countries have encountered similar problems; they all had to produce new programmes and applications or modify those already made that were adapted to the Microsoft environment, so they would also support other operating systems and be compatible with different formats, which only contributed to the increase of expenses (Souza, 2006).

There are some examples of transfers from the open source software back to the proprietary software. One such case occurred in Vienna when the users transferred back to Windows Vista and decided to develop their own distribution based on Debian Linux, called Wienux in 2005. In this case the major problem was a programme for computing education for children developed in 2003. It was developed only for the Internet Explorer environment and did not support the open source Firefox environment. The company that has developed the programme has foreseen the support for Firefox as late as in 2009. Therefore, in 2008, Vienna decided to go back to using Windows (Mobility, 2008).

The last such transfer was made by the German Ministry of Foreign Affairs that transferred to open source software in 2005. At the ministry they installed the Debian Linux distribution on their computers. The purpose of the mentioned transfer was to save the money that they would normally have spent on their licensed programmes. In their 2007 report they wrote that the transfer to open source software indeed helped them reduce their expenses. In 2011, they publicly announced that they are transferring back to MS Windows and MS Office. As a reason they stated that the programme did not support all hardware such as printers etc. In their opinion, expenses have not decreased, because they had to invest a lot of money in the development of their own printer drivers. The users have also complained regarding the lack of functions and poor interoperability. In their opinion, to transfer back to MS Windows will cost less, because they will not have to pay programmers to develop new drivers (http://tinyurl.com/5s4k3ry).

4 INFORMATION SECURITY AND THE ROLE OF OPEN SOURCE SOFTWARE

News about cybernetic attacks is becoming very frequent; most prominent are attacks between the USA and China. Nevertheless, cybernetic attacks are taking place also between numerous other states, since this asymmetric form of fighting allows them to reach targets with little effort and, what is even more important, without the use of force. However, these types of attack can have even greater consequences (Stuxnet example). Based on the McAfee report, over 120 countries have developed or possess "cybernetic weapons" for attacks on financial markets, state computers, military bases etc. These attacks are of various forms; from the DDOS attacks and hacking into systems to the theft of information. Due to an increased number of such attacks numerous countries have established special centres (in addition to CERT) to provide better communication between the affected individuals of an attack or to provide better response to such a situation. There is no uniform approach to the solving of this issue – each country has an approach of its own. The opinions on who should have the information about the attack and to what extent when such an attack occurs are also very diverse. Some believe that it is best to exclude the public, while others recommend as much transparency as possible (Baker, 2009).

Two approaches are predominant in the field of information security. The "top-down" approach derives from the concept of national security and is based on realistic security theory; it puts the state and its role in the writing and adopting of legislation, guidelines and strategies in the field of information security in the forefront. The security of individuals in the field of information and communication technology (ICT) must be taken care of by the state. However the state can also be directly or indirectly threatened by individuals (Svete, 2005). The weakness of such a system is that the legislation is falling behind the practice and that it is difficult for countries to protect individuals in the filed of ICT security in practice.

The "bottom-up" approach derives from the concept of human security, liberalistic and constructivist theory. This approach focuses on the individual, his values and interests. An individual in this field is not merely a victim that must be protected by the state, but an extremely important factor within the framework of information security who can have a strong influence on it through his work. An individual unskilled in the ICT domain can considerably threaten security. On the other hand, a very skilful individual can greatly contribute to security (Svete, 2005).

In the field of information security open source software can present a "bottom-up" approach, for it gives every individual an opportunity to control his own system. Even though its security is each individual's responsibility, the role of the open source community, which publicly warns about the threats, is likewise very important.

According to Diver (2007) an ideal system would be a combination of the "top-down" and "bottom-down" approaches. The state requires strategic guidelines and

legislation in the field of information security. Nonetheless, it would also be beneficial if they had individuals that would be more skilled in information science, who would take care of the system's security and thus prevent the spread of malware.

Conclusion

Throughout the years open source software has become serious competition for proprietary systems that hold a primary position both among supercomputers and servers. This increase has been noticed also by states, which have decided to transfer to open source software during the economic crisis with the desire to reduce costs, while other states decided for the transfer merely for security reasons and due to a desire for greater independence.

Security is relative. Each system can be hacked; therefore we cannot claim that one system is better than the other. Open source software has good security mechanisms, but in practice its safety depends greatly on its users. Open source software provides greater transparency and the possibility of insight into the source code, which interests only a small number of people. The majority of people use their computer for simple matters, such as writing documents. As far as security is concerned, people trust the developers of open source software and the many eyes system. But, in practice, it is evident that both systems are too much trust-based. There are a lot of cases where vulnerabilities in the systems have not been discovered for several years. Proprietary systems, on the other hand, do not allow an ordinary user to access the source code and are lacking the many eyes system. As with the open source software, here as well, security is based on the trust put into the developers. The only difference between open source software and proprietary systems is transparency. However, both systems are, unfortunately, based on the trust of people. Numerous countries have decided for open source software, because it allows them to inspect the source code themselves and, in addition, they can develop custom-made open source software. The main advantage of open source software in reference to proprietary systems is the public information about its vulnerabilities and their rapid elimination.

Open source software has good security mechanisms and provides greater transparency. Regardless, the endangerment of the system remains in the hands of the users. Most users are not skilled in using computers. These users endanger the security of their own and foreign systems, because they do not use antivirus programmes and do not update their computers regularly.

Hypothetically, in information security, open source software could be useful in the "bottom-up" approach only if all users were skilled in using computers, able to read the source code and detect vulnerabilities they could later publish publically. Since such expectations are utopian it is difficult to claim that open source software is better in terms of security because, at the end of the day, it is the user who presents a threat to the system.

Due to the current economic crisis in the world many countries are deciding to transfer to open source software to reduce costs. Slovenia is one of them. At this point it is necessary to draw attention to the possible challenges that might appear in case of a hasty and thoughtless transfer to open source software. We can learn a great deal from the German and Viennese examples (transfer back to proprietary systems because open source software did not support all hardware equipment). The compatibility of open source software and the current (or planned) hardware would have to be ensured. If established that such equipment is not supported, the costs pertaining to the development of appropriate drivers would have to be examined. The largest challenge probably lies in the software that is written only for the Windows environment. Therefore the costs for the development of corrections that would provide open source software support and the time for their production would also have to be examined. It would be reasonable to examine the current distributions and find the most appropriate distribution for the Slovenian environment (development of a local distribution is also possible).

If Slovenia does not start a possible transfer to open source software wisely it could happen that such a transfer will not be beneficial. In Slovenia, literature about this topic is scarce and so are articles and studies. In the future, it would be useful to carry out more independent cost-benefit analyses that would establish the advisability of Slovenia's transfer to open source software.

Bibliography

1. *Baker, S., 2009. In the Crossfire: Critical Infrastructure in the Age of Cyber War. Santa Clara: McAfee, Inc. http://tinyurl.com/3l6k4bm (3 August 2011).*
2. *Blanchard, J. F., 2007. China, multinational corporations, and globalization: Beijing and Microsoft battle over the opening of China's gates. Seoul: Asian perspective. Institute for Far Eastern Studies. http://tinyurl.com/3vb97m4 (2 April 2011).*
3. *Campbell, D., 1999. NSA Backdoor Into Windows. http://tinyurl.com/3k3e4d (12 April 2011).*
4. *Chuvakin, A., 2003. An Overview of Unix Rootkit. Chantilly: iDEFENSE Inc. http://tinyurl.com/42gbmjd (10 September 2011).*
5. *Cleto, S., 2004. Venezuela Embraces Linux and Open Source Software, but Faces Challenges. http://tinyurl.com/3dqh9ns (3 May 2011).*
6. *Diver, S., 2006. Information Security Policy - A Development Guide for Large and Small Companies. Washington: SANS Institute. http://tinyurl.com/3suc5tc (17 September 2011).*
7. *Espiner, T., 2006. Trend Micro: Open source is more secure. http://tinyurl.com/3c6u6cz (20 May 2011).*
8. *Espiner, T., 2010. Microsoft opens source code to Russian secret service. http://tinyurl.com/2w8moaq (3 August 2011).*
9. *Geer, D., in drugi, 2003. CyberInsecurity: The Cost of Monopoly How the Dominance of Microsoft's Products Poses a Risk to Security. http://tinyurl.com/63bhse8 (18 September 2011).*
10. *Germain, J. M., 2008. Linux: A Tempting Target for Malware?. http://tinyurl.com/65jn5vu (1 May 2011).*
11. *Gonzalez-Barahona, J., Robles, G., 2006. Libre Software in Europe. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 161–188.*
12. *Humbery, B., 2011. The Evolution of the Personal Package Archive system. http://tinyurl.com/3tqw8rq (20 May 2011).*

13. *Jose, M., 2011. The Goal is 200 Million Ubuntu Users in 4 Years - Mark Shuttleworth at UDS. http://tinyurl.com/3cd4p67 (23 May 2011).*
14. *Kalkuhl, M., 2009. Malware beyond Vista and XP. http://tinyurl.com/3qemfbs (20 May 2011).*
15. *Kimberly, S., 2005. The value of open standards and open-source software in government environments. Austin: IBM SYSTEMS JOURNAL. Volume 44 Issue 2, January 2005. http://tinyurl.com/3qsatqt (12 May 2011).*
16. *Koetzle, L., 2004. Is Linux More Secure Than Windows? http://tinyurl.com/3p9uue8 (20 May 2011).*
17. *Kovačič, M., 2006. Kriptografija, anonimizacija in odprta koda kot boji za svobodo na internetu. Javnost- the public. Vol. 13. (2006). Fakulteta za družbene vede, Univerza v Ljubljani, p. 93–110.*
18. *Laurie, B., 2006. Open Sources and Security. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 57–71.*
19. *Lewis, J., 2006. Government Open Source Policies – August 2007. Washington: Center for Strategic and International Studies. http://tinyurl.com/3mhva3y (12 May 2011).*
20. *Lock, B. Y., Liu L., Saxena S., 2006. When China Dances with OSS. V C. DiBona, ed. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 197–210.*
21. *Meintjes, T., 2011. Is a virus or malware infection the cause of your slow computer? http://tinyurl.com/442u5se (26 May 2011).*
22. *Mihajlovič, N., 2011. Microsoft gre nad Pahorja, zdaj hoče pošteno konkurenco. http://tinyurl.com/3lxz4va (24 May 2011).*
23. *Mobility, T., 2008. Vienna failed to migrate to GNU/Linux: why?. http://tinyurl.com/6mktzl (9 September 2011).*
24. *Morozov, E., 2011. A Walled Wide Web for Nervous Autocrats. http://tinyurl.com/2vflb3c (29 May 2011).*
25. *O'Dowd, D., 2004. Linux Security Controversy. http://www.ghs.com/linux/security.html (18 September 2011).*
26. *Peeling, N., Satchell, J., 2001. Analysis of the Impact of Open Source Software. http://tinyurl.com/6lyeod8 (19 May 2011).*
27. *Poulsen, K., 2001. Borland Interbase backdoor exposed. Open source reveals foolishly hardcoded password. (12 May 2011).*
28. *Proffitt, B., 2002. Venezuela's Government Shifts to Open Source Software. http://tinyurl.com/3j9kqzo (15 May 2011).*
29. *Sapronov, K., 2007. Kaspersky Security Bulletin 2006: Malware for Unix-type systems. http://tinyurl.com/3vuu2k3 (23 May 2011).*
30. *Saxenian, A., 2003. Government and Guanxi: The Chinese Software Industry in Transiton. Berkeley: University of California at Berkeley. http://tinyurl.com/3u37nwl (12 May 2011).*
31. *Schneier, B., 2002. Secrecy, Security, and Obscurity. Crypto-Gram. http://tinyurl.com/5rk6jaw (17 May 2011).*
32. *Schneier, B., 2006. Microsoft Vista's Endless Security Warnings. http://tinyurl.com/ges4k (23 May 2011).*
33. *Souza, B., 2006. How Much Freedom Do You Want. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 211–229.*
34. *Svete, U. 2005. Varnost v informacijski družbi. Ljubljana: Fakulteta za družbene vede.*
35. *Weber, S., 2004. The success of open source. Cambridge: Harward University Press.*
36. *Wynants, M., 2005. Free as in Freedom, not Gratis!. V Wynants, M., Cornelis J., ed. How Open is the Future? Economic, Social & Cultural Scenarios inspired by Free & Open-Source Software. Brussels: Brussels University Press, p. 69–85.*

Sources

1. *http://distrowatch.com/ (26 May 2011).*
2. *http://librenix.com/?inode=21 (23 April 2011).*
3. *http://support.apple.com/kb/ht1528 (26 May 2011).*
4. *http://tinyurl.com/27l5wvh (26 May 2011).*
5. *http://tinyurl.com/28lpgq (28 May 2011).*
6. *http://tinyurl.com/3f69g8u (19 May 2011).*
7. *http://tinyurl.com/3fldnhr (26 May 2011)*
8. *http://tinyurl.com/3hdqvgd (20 May 2011).*
9. *http://tinyurl.com/3pdksvv (20 May 2011).*
10. *http://tinyurl.com/44x9pxd (26 May 2011).*
11. *http://tinyurl.com/5s4k3ry (10 September 2011).*
12. *http://tinyurl.com/68u2cm7 (12 April 2011).*
13. *http://tinyurl.com/6gyjnou (20 May 2011).*
14. *http://tinyurl.com/6hszcy5 (20 May 2011).*
15. *http://tinyurl.com/6jgg3ut (20 April 2011).*
16. *http://tinyurl.com/hdpo9 (18 September 2011).*
17. *http://tinyurl.com/o4foa (3 May 2011).*
18. *http://www.Linuxfordevices.com/ (20 April 2011).*
19. *http://www.osor.eu/about (20 May 2011).*
20. *https://bugs.launchpad.net/ubuntu/ (18 September 2011).*

Anže Rode,
Kristian Bernšak,
Bojan Langerholc

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.5

Strokovni članek

ENOTA ZA SPECIALNO DELOVANJE SLOVENSKE VOJSKE – ODGOVOR NA SODOBNE IZZIVE

THE SAF SPECIAL OPERATIONS UNIT RESPONSE TO MODERN CHALLENGES

Professional article

Povzetek Enota za specialno delovanje (ESD zagotavlja zmogljivosti specialnega delovanja Slovenske vojske in uresničevanje posebnih nacionalnovarnostnih ciljev Republike Slovenije.

Visoka usposobljenost, sposobnost prikritega delovanja, zmožnost velike natančnosti zaradi zmanjševanja stranskih učinkov in visoka prilagodljivost glede na različne vire ogrožanja so samo nekatere značilnosti, ki poudarjajo vlogo in pomen ESD znotraj oboroženih sil. Te značilnosti omogočajo njeno uporabo za izpolnjevanje obveznosti Republike Slovenije do sistema kolektivne obrambe zveze Nato ter zagotavljanje mednarodne varnosti znotraj OZN v mednarodnih operacijah in na misijah, ko drugih enot ter virov Slovenske vojske ni mogoče uporabiti. Hkrati je ESD potencialna zmogljivost za obrambo države in delovanje v posebnih kriznih razmerah protiterorističnega delovanja v Republiki Sloveniji.

ESD je s potrditvijo svojih zmogljivosti v praksi pokazala, da so predlagani teoretični koncepti in rešitve, na katerih temelji, pravilni in uresničljivi, ESD pa vrhunsko usposobljena enota, ki predstavlja ost enot za bojno delovanje Slovenske vojske.

Ključne besede ***Specialno delovanje, protiterorizem, protiuporništvo, Nato, Enota za specialno delovanje, na učinkih temelječe operacije.***

Abstract The Special Operations Unit (SOU provides special operations capabilities for the Slovenian Armed Forces (SAF and the implementation of special national security objectives for the Republic of Slovenia.

Specialized training, the ability to perform covert operations, high accuracy to achieve collateral damage reduction, and great flexibility in facing different sources of threat are but a few of the features that highlight the role and importance of the Special Forces units of the armed forces. Having such characteristics, the unit can be used to fulfil the obligations of the Republic of Slovenia to NATO's collective defence system and ensure the international security of UN missions when no other SAF units and capabilities can be employed. At the same time, the SOU provides

potential capabilities for national defence and specific crisis situations for counter-terrorism activities in the Republic of Slovenia.
By validating its capabilities in practice, the SOU has shown that the theoretical concepts on which it is based are both good and feasible. It has proved itself to be a highly qualified unit – the elite of the SAF's combat operations units.

Key words ***Special Forces, special operations, counter-terrorism, counter-insurgency, NATO, Special Operations Unit, effects-based operations.***

Introduction

The changing nature of threats and conflicts in the post-Cold War era and the projection of the security environment require countries and organisations (such as the UN, EU and NATO) to have a different and particularly more effective way of facing these challenges[1]. Indeed, the threats and challenges have important implications and have required significant changes to security systems and armed forces, including special operations forces.

The Resolution on the General Long-Term Development and Equipping Programme of the Slovenian Armed Forces up to 2025 (2010, p. 7) states that:

"... the likelihood of an interstate armed conflict in the Euro-Atlantic region has diminished significantly. Military threats will mainly emerge as local and regional instabilities which can easily spill over. Moreover, contemporary threats are increasingly becoming hybrid in their form, and multi-layered and international in nature under the influence of strong globalisation effects. In addition to land, sea and air, the theatre of the future will also include cyberspace and space."

The authors thus believe that the future security environment will become even more complex due to a combination of different elements: the greater lethality of modern weapons, the development of means for a more rapid deployment of military forces, international terrorism[2], the proliferation of weapons of mass destruction, easier access to information, the presence of the media etc. The military structures and methods[3] suitable for resolving international conflicts will not be able to manage complex 21st century security situations.

---

[1] *The prevailing view among different global defence and security entities is that our present and future security environments represent new complex challenges that are difficult to predict. Different and »unconventional« threats can compromise wider international stability and cause a permanent state of conflict. Special Forces are an active instrument that is ideally adapted to a non-defined and dynamic environment, while maintaining freedom of action by applying the economy of forces principle. In addition, special operations forces have a special ability to complete their tasks in environments where conventional forces are in a worse strategic or operational position (NATO Special Operations Study, 2008).*

[2] *Terrorism epitomizes contemporary asymmetrical threats. In this context, Prezelj states (2007, p. 67) that "asymmetry refers to the disproportionality of the entity which threatens (non-state actors against the state) the resources it uses, and the consequences (minimum input – maximum output outcome) which, for example, exceed the direct consequences of a bomb explosion)".*

[3] *Naturally, the SOU is but a segment of a comprehensive response to terrorism by modern countries (Prezelj, 2007, p. 68) which enhances joint activity and the country's response (the overall picture).*

The Mid-Term Defence Programme (hereinafter: SOPR) for 2007–2012 (2006) indicates that the future strategic security environment shall be significantly affected by: globalisation, sophisticated lethal weapons and various forms of asymmetric warfare, rapidly changing security situations, demographic and political factors and the lack of resources that cause mass migrations, the spread of radical ideologies, unresolved international and internal conflicts and major natural disasters. The SOPR for 2007–2012 also anticipates that globalization will make the Western democracies, in particular their economies, even more sensitive to stability in different parts of the world, which will directly or indirectly affect their economic interest and open market operations.
Information networks already enable us to get a real-time overview of events over the world. In the future, this will be exploited by different actors employing IT-strategies, also by those whose main purpose is destruction. Increasing access to modern and advanced technologies will make terrorist and other attacks more effective. The direct threat of possible access to technologies and means of mass destruction sponsored by states will also become increasingly prominent (SOPR for 2007–2012).

The gap between developed and developing countries will continue to cause ethnic conflicts and mass migration. Economic and financial crises will build up pressure and contribute to the collapse of social systems (SOPR for 2007–2012).

There will be an increase in requirements for water, food and energy resources and climate changes will have a negative impact on water and food supplies. Environmental degradation will likely result in an increased number of natural disasters which will have long-term effects on some of the world's social and economic conditions. There will also be an increase in organised crime and poverty. New diseases will emerge and famine will strike (SOPR for 2007–2012).

The threats will be posed by unstable states, the poor management of resources and constant competition for them. Unresolved conflicts as well as groups and countries supporting radical ideologies will represent threats which could gain global dimensions. Thus, some severe forms of the threats in question might shake the foundations of global stability (Rode, 2007, p. 5).

There is the possibility of strategic surprise, which will come with little or no prior warning. For this reason, participation in the NATO Alliance will be important and will present a reasonable possibility for the activation of a collective defence.

The situation in the Balkans will remain unstable. Kosovo, in particular, will continue to be problematic. Nevertheless, international forces which ensure stability in Kosovo and Bosnia and Herzegovina will be restructured and reduced in number. At the same time, the process of integrating the Southern Balkan countries into NATO and the EU will continue.

The security situation in Africa will continue to be critical, and will be influenced by various factors, such as rapid population growth, epidemics, poverty, famine, water shortages, unstable regimes, failed states, interreligious and interethnic tensions etc. These factors and the situations they create will result in illegal migrations to Europe and the proliferation of terrorist groups that focus their operations on Europe (SOPR for 2007–2012). So far, the so-called "Arab Spring" in Tunisia, Egypt, Libya and elsewhere has not confirmed these pessimistic forecasts.

The Middle East will remain a crisis area. Interethnic and interreligious conflicts with terrorist operations will continue and with a potential focus on European countries (SOPR 2007–2012).

The spectrum of future warfare will be focused on crises in which nuclear and other weapons of mass destruction could be used, on classic inter-state conflicts, internal conflicts resulting in the collapse of countries, on terrorism and other crisis situations. A particular challenge will be the fact that the different dimensions of war include not only the armed forces, but also different actors: national, international, non-governmental and local as well as elements of various instruments of power, such as political, military, informational and economic.

The state usually responds to military threats with its armed forces. Similarly, as part of the continued Alliance integration process, the SAF's units will assume increasingly important commitments, not only in terms of the size and number of participating units, but also in terms of the complexity and difficulty of the tasks assigned.

1 NATO, THE SLOVENIAN ARMED FORCES AND SPECIAL OPERATIONS FORCES

Based on lessons learned and experiences gained, especially in special forces operations in Afghanistan, a decision was made at the NATO's 2006 Riga summit regarding NATO's Special Operations Forces Transformation (NATO SOF Transformation Initiative). This had the purpose of achieving greater comparability and capability for joint operations through common training, equipping, and introducing and meeting common standards. For this purpose, NATO's SOF Coordination Centre (NSCC) was established in 2007 (Special Operations Headquarters (NSHQ) since the beginning of 2010). This centre has become the single body for the management and coordination of NATO's special operations. It optimises the employment of Special Operations Forces by the Alliance and provides operational command facilities in accordance with the SACEUR guidelines (see Beršnak, 2010, pp. 27–28).

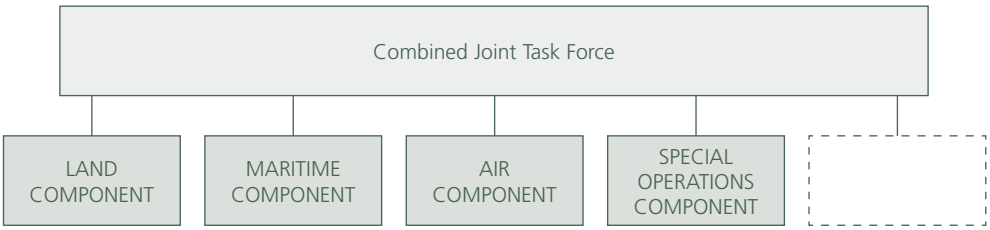
According to Paternus (2010, p. 70), the North Atlantic Council adopted the document MC 437/1 Special Operations Policy in 2006 as a starting point for the establishment of common standards. The document forms the foundation for the development of NATO's joint doctrine for special operations. In 2008, the ratification

process of the AJP 3.5, Allied Joint Doctrine for Special Operations, was initiated. This process was completed in 2009, when the document was ratified as the SVS STANAG 2523(1).

In fact, the documents in question, i.e. the MC 437/1 Special Operations Policy and the AJP 3.5, define the significance and purpose of the special operations forces in national and collective defence and represent the two most important documents related to special operations forces.

The Military Doctrine of the Slovenian Armed Forces defines special operations forces as one of the components of the Combined Joint Task Force (CJTF) (Fig. 1), which is organised according to its mission, joint operations area, and main mode of operation. In addition to the special operations component, the CJTF includes land, maritime and air components (see Furlan et al., 2006, p. 29).

Figure 1: Combined Joint Task Force (Furlan et al. 2006, p. 29)



The SAF Special Operations Forces assume the leading role in special operations, which are a form of combat operations carried out by specially selected, equipped, organised and trained SAF units in support of military, political or psychological objectives of operational or strategic importance. They comprise non-conventional forms of combat operations, direct actions, special reconnaissance, intelligence, counter-terrorist actions, psychological operations and combat search and rescue. They are oriented towards military targets (Furlan et al., 2006, p. 50). According to the definition given in the Military Doctrine (Furlan et al. 2006, p. 50-51), the SAF Special Operations Forces will typically operate in small groups, independently, deep behind enemy lines, over prolonged periods of time and under cover. They carry out their tasks in support of SAF offensive, defensive and information and stability operations. Should the enemy occupy and control part of the Republic of Slovenia's territory, SAF special and other forces will carry out non-conventional forms of combat operations with an emphasis on guerrilla tactics. The units will regroup into smaller groups the aim of which is continuous disruption, destruction, neutralisation and minimising the enemy's morale. Combat operations will be conducted independently, in a covert and resourceful manner, continuously, thus forcing the enemy to refrain to static battle formation and expanding the terrain for the manoeuvre of SAF units. The units avoid frontal engagement. Combat operations in an occupied terrain are based on aggression and surprise.

2 NATO SOF TASKS

2.1 NATO SOF principal Tasks

The SVS STANAG 2523(1), Allied Joint Doctrine for Special Operations defines the principal tasks of NATO's Special Operations Forces (hereinafter: tasks) as follows:

- **Special Reconnaissance (SR)** is an information gathering activity which complements national and Allied intelligence collection sources and systems by obtaining specific, well-defined, and time-sensitive critical information at the operational and strategic levels. When the reconnaissance and intelligence authorities of conventional forces are constrained by e.g. high enemy activity, difficult terrain, and are thus unable to provide precise and time sensitive data, special forces are employed;
- **Direct Actions (DA)** complement NATO capabilities with strikes on specific, precisely-defined targets of strategic or operational significance. Direct actions are limited in scope and time. The main modes in the conduct of their operations are: Raids, Ambushes, and Direct Assaults, Terminal Guidance Operations, Recovery Operations, Precision Destruction Operations, Armed Reconnaissance and Opposed Boarding Operations;
- **Military Assistance (MA)** includes a wide range of support activities to friendly forces. In the context of military assistance, Special Forces can assist in training, equipping, providing support and employment (operation).

Figure 2 shows the concept of the SOF's principal task allocation and the relations among them in the performance of those tasks during the conflict, while Figure 3 shows a basic spectrum of task performance in the context of NATO's crisis management system.

Figure 2: NATO SOF and the spectrum of conflict (Newton 2010)

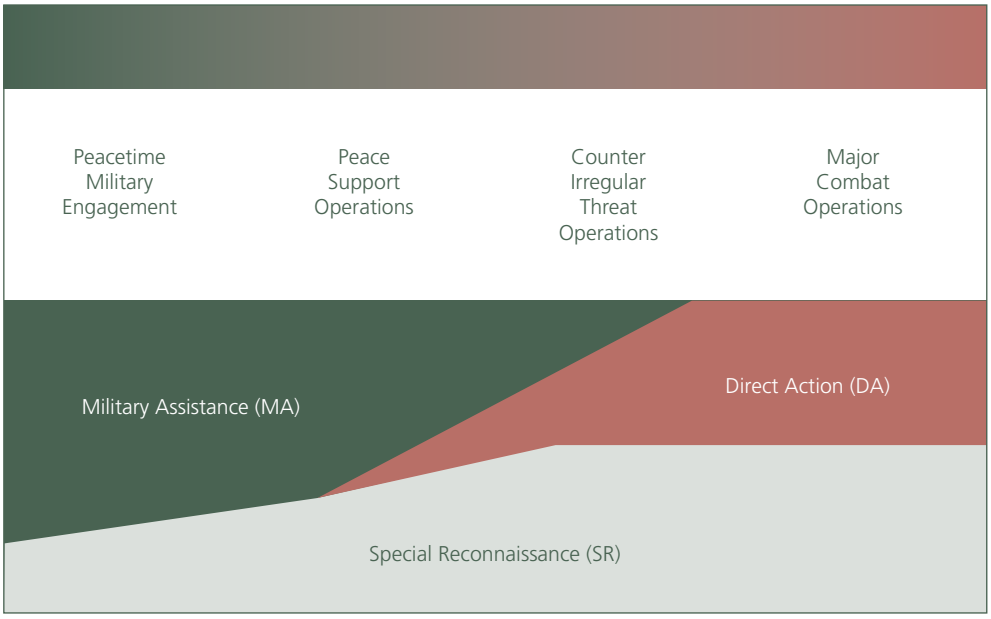
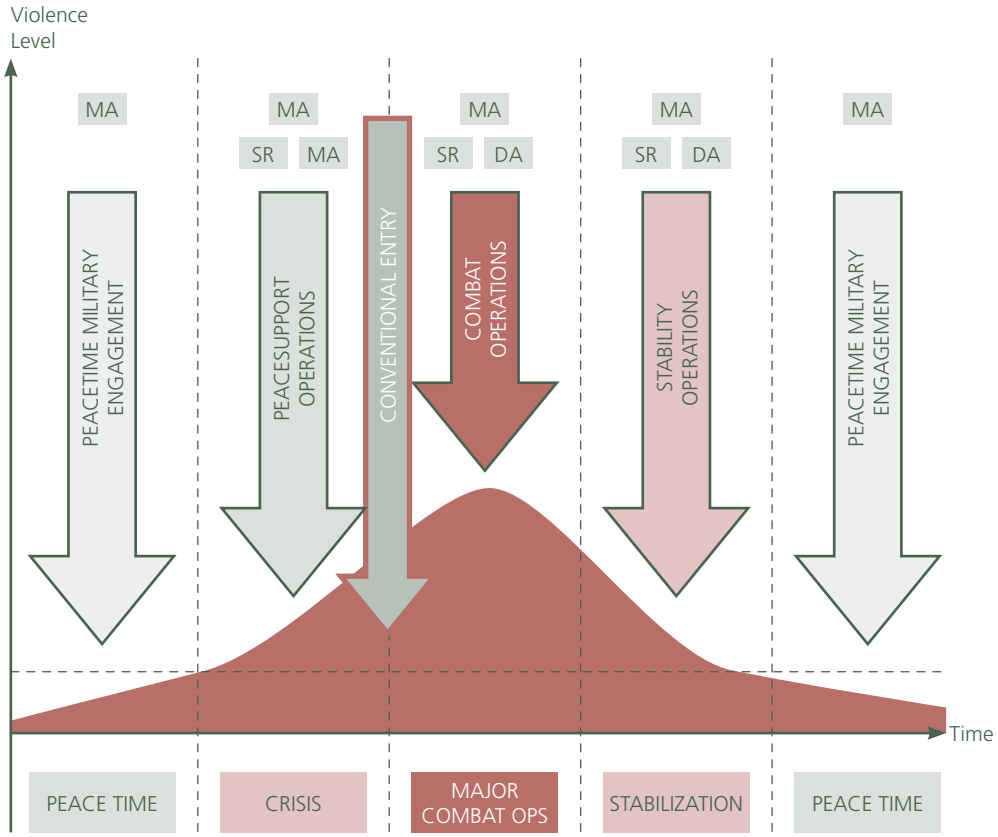


Figure 3: NATO Crisis Management System and SOF Tasks



2.2 Other SOF Tasks

In addition to the SOF's principal tasks, there are other tasks defined in the SVS STANAG 2523(1) which involve (but not exclusively) the participation of NATO's special operations forces, namely:

– support to counter irregular enemy operations and counter-terrorism[4] and counter-insurgency[5] operations in the context of the Alliance operations;
– hostage rescue operations – the SOF can assist in these operations under special conditions.

It should be stressed that the SOU, despite its capabilities, has no statutory powers to perform such activities in the Republic of Slovenia. Statutory powers rest with the Special Task Unit of the Police and the SAF's Military Police in military facilities and areas (Defence Law).

[4] *Counter-terrorism as one of the SOF's tasks is defined in the Military Doctrine (2006: 50) and the Directive of Organisation and Operation of the SAF's Special Operations Forces (2008: 4).*

[5] *Counter-insurgency as a form of special operations is defined in the Directive of Organisation and Operation of the SAF's Special Operations Forces (2008: 4) as "support to Counterterrorism and Counterinsurgency".*

In their final definition, the SAF's SOF tasks will have to be clearly defined and comply with the definitions set out in MC 437/1 and AJP 3.5. This refers particularly to additional tasks which involve the possible participation of SAF Special Forces. Participation is determined on the basis of statutory powers.

3 SPECIAL OPERATIONS TASK UNIT

All concepts and standards applicable to the SAF and NATO are reflected in their capabilities and are defined in force goals for individual countries. The SAF's force goals are that the SOU provides the Special Operations Task Unit (SOTU) for NATO. The SOU is organised in such a way as to provide several Special Operations Task Units.

NATO defines the capabilities of and the differences among Special Operations Task Units. Thus, the SOTU of the SOU includes command and control, combat, and combat service support elements. From this starting point, the combat unit has the following capabilities:

- planning and conducting special operations in hostile environments, either independently or as an integral part of a larger formation, with other military and security structures or allied or host nation forces;
- conducting the full spectrum of special operations, depending on special approvals;
- deployment and redeployment within planned time frames, all classes of supply included;
- ground, air or water infiltrating and exfiltrating;
- conducting special operations in remote areas or hostile environments for a longer period of time and with the minimal external support;
- performing tasks in subgroups;
- day/night reconnaissance and target control, carrying out control in vehicles and on foot;
- carrying out limited attacks from a distance using sniper weapons and man-pack explosive devices;
- performing manoeuvre operations employing tactical means of transportation and collective support weapons;
- terminal guidance operations;
- developing, organising, training and advising or guiding military and/or paramilitary host nation forces – with attached translation capabilities.

The complexity of tasks and the conditions in which SOU members operate necessitates different equipment from that of other units. Owing to the various forms and circumstances of operations, SOU members have several special purpose kits and armaments.

4 EFFECTS BASED OPERATIONS CONCEPT

The concept of *Effects-Based Operations* (EBO) was introduced in the U.S. air forces at the tactical level during the First Gulf War. It refers to the planning and conducting of combat operations by combining military and non-military methods to achieve effects. The concept was developed to take advantage of the significant progress in military technology and tactics, whereby the commander's purpose could be achieved causing minimal collateral damage and posing minimal risk to their own forces (Batschlet, 2002).

The concept was later tested at the strategic and operational levels, but was officially dropped from common usage due to different interpretations and owing to the belief that it gives the commanders a false sense of predictability (Mattis, 2008). It was replaced by the *Comprehensive Approach Concept*. According to many critics (Vego, 2006; Mattis, 2008; Riper, 2009; see also Smolej, 2011), the concept is useful especially in terms of targeting at the tactical level. Despite being no longer used at the higher levels of command, the concept still presents a useful tool for goal achievement at the tactical level. On the basis of large amounts of intelligence, special operations forces have more leeway in target identification processes, especially where the EBO concept is used to guide their operations in terms of achieving specific effects.

This usually means that in practice, commanders of SOF units primarily focus on asymmetrical battlefield targets for which they have sufficient, quality intelligence[6]. These targets can be covertly monitored and controlled (Small Footprint) by the commanders themselves, and neutralised with great precision at a selected moment. On the other hand, lower tactical unit commanders of conventional forces mainly use their forces to show the force in order to deter the enemy from its intentions (Big Footprint). Upon coming across the enemy[7] in the conduct of their missions, they will try to keep contact with it and destroy it with reinforcement (Figure 4).

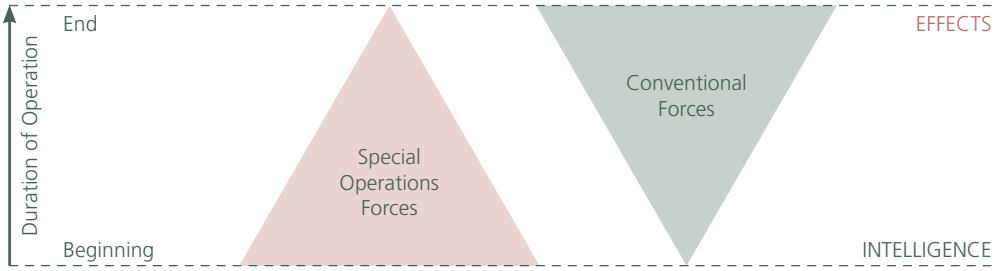


Figure 4: The difference between the Concept of Operations for Special Forces and Conventional Forces

[6] *In our opinion, so-called anti-head operations can be controversial and counterproductive if carried out in a careless manner, since it may give an additional spur to insurgency. This is also reflected in the case of the transfer of General Petreus's strategy from Iraq to Afghanistan, which has not brought the desired effects (see also Svete, Guštin, Črnčec, 2011).*

[7] *Physical contact of intelligence.*

The effects should be examined from two perspectives: at the tactical level, the effect is primarily associated with damage caused to the enemy. At the operational level, the effect is assessed in terms of wider impacts on a certain geographical and social environments.

Smith (2006) observes that future conflicts and engagements will take place between civilian populations. However, the main actors of conflict will include differently organised forms[8] rather than countries and their armed forces. The operations of their armed forces following conventional military principles will bring unnecessary casualties and further resistance.

A military operation may be successful in tactical terms, but its performance might be counterproductive at the operational level. This means the loss of trust, and failure to achieve centres of gravity[9].

This is often the case in counter-insurgency (COIN), in which the enemy's operation primarily depends on local support (Celeski, 2005). Thus, military operations[10] that have otherwise been successful at the tactical level might shift the focus of sympathy to the enemy. This is due to side effects among the civilian population and on civilian infrastructure, or due to disapproval of local communities, which, at the operational level, demands much more effort and time to create a secure environment.

For the reasons stated above, the motto of SOF combat operations is: *"Think operationally, act tactically"*. It should be stressed that in counter-insurgency operations special operations forces (in comparison with the conventional ones which primarily perform kinetic operations[11] (Smith, 2008)), should primarily perform non-kinetic operations. This means that they can perform tasks related to psychological operations, civil-military cooperation and military assistance to achieve their goals. The U.S. special operations forces rediscovered the concept of *"Village Stability Operations"* (VSO) in 2009, which had been employed during the Vietnam War. The main feature of this concept is that minor groups of special operations forces are accommodated in key villages or settlements and as good neighbours, they help local communities in solving their problems. This help can vary from the provision of a

---

[8] *In this context, we can come across a network organization of terrorists/enemies that could also be characterized as organizational asymmetry. Organizational symmetry has always played an important role in the history of warfare. Innovations gave the actors a great advantage, even if they had no technological or other advantages. Similarly, Svete argues that "... governmental institutions will face network-organized non-state opponents rather than hierarchically-organized ones as is the case with the majority of governmental institutions in the area of national security (2007, p. 13).*

[9] *Terrorists/insurgents/enemies attack people who are the point of focus (POF), whereby their tactical operation creates a strategic impact. The Centres of Gravity (COG) are defined as features, capabilities or sites, from which a country, alliance, military force or other group draw from the freedom of their actions, physical strength or the will to fight. These points exist at the tactical, operational and strategic levels and represent the centre of power or operation, on which everything depends. They are also the point where all the energy is focused to achieve the objective. From this point arises the enemy forces' ability, power, and will. Their destruction or neutralisation brings a decisive advantage and victory.*

[10] *Successful in terms of linear battlefields, whereby the main goal is to cause damage to the enemy.*

[11] *The term 'Kinetic Operation' refers to combat operations, where physical strength is used.*

secure environment to assistance in establishing local self-government[12] and critical infrastructure which is important for the normal functioning of a social environment. One of the key tasks of Special Forces units operating this way in Afghanistan is to establish a link between local self-government and the Government of the Islamic Republic of Afghanistan (GIRoA).[13]

The EBO concept is important for the SOU in that it dictates the contents of the training process with regard to other SAF units. This training process has to refer both to the individuals and the unit. The SOF units must have greater generic capabilities for obtaining intelligence, and more robust analytical processing capabilities to operate in accordance with the EBO concept. Moreover, they have to be adaptive, since special operations units (being small in terms of personnel) may have a wider spectrum of capabilities, even in comparison with larger conventional units. This should be, among other things, a result of the selection procedures for manning these units, for they ensure manning with competent personnel (see Spulak, 2007, p. 20).

5 CONFIRMATION OF HYPOTHESIS

According to NATO doctrines of joint special operations forces, their development and equipping, all armed forces must have their special operations forces verified and tested.

Since 2004, the SOU has participated in international operations in which the SAF completes practical tests of its doctrinal solutions. Thus, the SOU was the first SAF unit to perform tasks in Afghanistan, Chad, the Lebanon and Iraq under NATO, EU and UN operations.

It should be noted that the SOU's tasks in Afghanistan are primarily tasks of military assistance (from 7 SVNKON ISAF–OMLT[14], NTM–I[15]) and partly reconnaissance operations (e.g. Afghanistan SVNKON 1 and 2 ISAF, SVNKON 1 UNIFIL in Lebanon, SVNKON 1 in Althea, and SVNKON 1 in Chad). The SOU also conducted combat search and rescue (Afghanistan SVNKON 1 and 2 ISAF) and information operations (INFOOPS, SVNKON 11 ISAF) in Afghanistan. The SOU has not participated in any direct actions, due mainly to the type of tasks undertaken by the SAF, and national caveats. Despite the fact that the SOU has not participated in direct actions, it has gained valuable experience and proved itself in the most demanding of environments. Modern special operations forces increasingly give attention to tasks related to military assistance and special reconnaissance, including human

[12] *Especially in terms of local security services.*

[13] *For more, see the above mentioned book that analyses counter-insurgency operations of the occupation forces in Slovenian territory during World War II.*

[14] *Despite all the merits of the SVNKON 14 ISAF which started to mentor the Afghan National Army battalion in 2010, it should be pointed out that the SOU had already provided training to the Afghan National Army in 2006. The SOU members also provided training to the Iraqi Armed Forces during the NTM–I mission in 2006.*

[15] *NTM – I: NATO Training Mission – Iraq.*

intelligence. As stated by Paternus (2010, p. 64), the ISAF operation is a test of readiness and training level, not only that of the SOU, but also of the Slovenian Armed Forces as a whole, which was participating in military operations outside of South Eastern Europe for the first time. In addition, operation in a desert environment more than 6,000 km away presents an enormous professional and logistical challenge, both for the SOU members, as well as the Slovenian Armed Forces. In a comparison analysis of NATO's SOF units in the military operation *Enduring Freedom,* Paternus (2010) identified comparability with SOU ISAF tasks, which included:

– long range reconnaissance and intelligence operations,
– combat search and rescue operations,
– search and destruction of arms and ammunition caches and
– the training of allied force members.

Lessons learned from the tasks performed by SVNKON 1 and 2 ISAF indicate the ability of the SOU to operate in accordance with NATO standards (e.g. AJP 3.5). Given the complexity and effectiveness of the tasks and a record of no incidents or injuries, Paternus (2010) observed that the SOU's members were properly equipped, trained and prepared for special operations. His findings were also supported by SVNKON 14 and 15 ISAF – OMLT operations, which included the participation of SOU members.

In the NTM–I operation, SOU members trained Iraqi security forces members through military assistance. Their tasks were performed at the Iraqi military academy in Al Rustamiyah and were similar to those of SVNKON 7 ISAF – OMLT members, whereby the provision of security presented an even greater challenge. Despite the cultural differences between the members of the Afghan and Iraqi security forces, SOU members demonstrated an adequate level of cultural awareness and the ability to operate in a foreign cultural and social environment, which is one of the fundamental features of special operations forces.

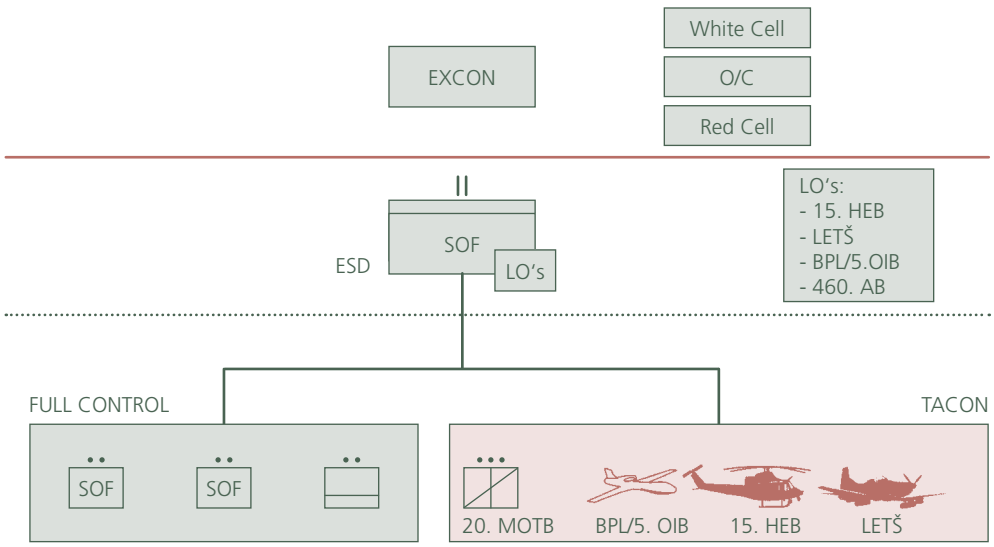
The SOU gained similar experience in CAR / Chad and UNIFIL operations while deployed in remote and rough desert areas. The tasks performed by the members for brigade-level units could be characterized as special reconnaissance as they operated in light armoured vehicles. The level of self-supply was high, which is significant given the ISAF operation. A great challenge was off-road vehicles which require a larger radium, a desert environment, while the protection against improvised explosive devices (IED) was of lesser significance, at least in operations in Chad. Both operations, although under the EU and UN auspices, have confirmed the concepts of unit training as regards the task accomplishment. The doctrinal and conceptual solutions, arising from the SVS STANAG 2523(1) proved to be appropriate for these operations.

The entire scope of tasks (direct actions, special reconnaissance and military assistance), for which the SOU is trained, has been tested in tactical exercises as well.

Thus, training and exercises are conducted prior to their use in real combat in order to test the theoretical concepts and solutions. The SOU tested its conceptual solutions and capabilities for the implementation of mission essential tasks at the *RIS 2011 Tactical Exercise* .

Its main purpose was to test the SOU Special Operations Task Unit (SOTU) while conducting special operations in support of counter-insurgency operations. They operated in the asymmetric battlefield conditions in which the SAF's ISAF units in Afghanistan have currently been deployed. Another purpose of the exercise was to test SOTU's capabilities for joint combat operations (Figure 5). This produces synergistic effects (1 + 1 = 3) which enable Special Forces to have relative superiority (McRaven, 1995) in space and time over a numerically stronger enemy.

Figure 5: Force Organisation of the RIS 2011 Exercise Elements



Conclusion

International operations as well as at the RIS 2011 tactical exercise have proved the SOU to be a highly trained unit and the elite of SAF combat operations units. The unit has tested and confirmed, in practice and on exercise, the capability of conducting special operations and **combat joint operations** in support of COIN operations in asymmetric battlefield conditions, in which the SAF's ISAF units have currently been operating. Furthermore, by verifying its capabilities in practice, the SOU has shown that the proposed theoretical concepts and solutions underlying its operation are correct and feasible. It reaffirmed its commitment to excellence and exceeding the standards. The sayings such as the quality is more important than the quantity; a man with his knowledge and experience is more important than his equipment; and members of special forces cannot be trained in a short time, even if this be necessary, have proved true again.

The Republic of Slovenia has committed itself to have developed and prepared the SOTU, represented by the Special Operations Unit in accordance with the SAF's development plans within force goals by 2012. The SOU has achieved its goal within the limits of its competence and capabilities. This is confirmed by deployments in international operations, exercises and the personal experience of authors. For complete integration into NATO's special operations forces, it is necessary to determine the framework nation. This important issue, however, lies outside the SOU's competence.

A systematic and comprehensive approach to the establishment of the SOU provides capabilities for the SAF's special operations forces and special national and security objectives for the Republic of Slovenia. The training and equipping of special operations units is a long-term process, which should be given enough attention by the state and the armed forces in terms of the provision of human and material resources.

Specialized training, the ability to perform covert operations, high accuracy to achieve collateral damage reduction, and great flexibility in facing different sources of threat are but a few of the features that highlight the role and importance of the Special Forces units of the armed forces. Having such characteristics, the unit can be used to fulfil the obligations of the Republic of Slovenia towards NATO's collective defence system, and ensure international security in international operations and on UN missions when no other SAF units and capabilities can be employed. At the same time, the Republic of Slovenia acquires capabilities for the country's defence and operations in specific crisis situations[16] of counter-terrorism activity in the Republic of Slovenia.

Bibliography

1. *AJP-3.5. Združena zavezniška doktrina specialnih operacij (the original of January 2009, the Slovenian SVS STANAG 2523(1), July 2009). Ljubljana: MO RS.*
2. *Batschelet, A. W., 2002. Effects-Based Operations: A New Operational Model? Strategy Research Project, U.S. Army War College. http://www.iwar.org.uk/military/resources/effect-based-ops/ebo.pdf, 5. 5. 2011.*
3. *Beršnak, K., 2010. Preoblikovanje vloge in načinov delovanja enot za specialno delovanje zveze NATO v povezavi z evolucijo tipologije vojskovanja. Diplomsko delo, Maribor: Fakulteta za varnostne vede.*
4. *Celeski, J, D., 2005. Operationalizing COIN. Joint Special Operations University (JSOU) Report 05-2.*
5. *Furlan, B.; Rečnik, D.; Vrabič, R.; Maraš, V.; Cerkovnik, J.; Špur, B., Šonc, M.; Tušak, M.; Ivanuša, M.; Gorjup, B.; Kojadin, M.; Lasič, K. in Unger, M., 2006. Vojaška doktrina. Ljubljana: Defensor.*
6. *Mattis, J. N., 2008. USJFCOM Commander's Guidance for Effects-based Operations. Parameters, Vol. XXXVIII, Spring 2008. pp. 18–25. http://www.carlisle.army.mil/usawc/Parameters/Articles/08autumn/mattis.pdf, 9. June 2010.*
7. *Newton, R., 2010. Introduction to Special Operations. What makes SOF special. Power Point predstavitev, Chievres: NATO SOF.*

[16] *The employment of military capabilities for combat operations on the declaration of state of emergency.*

8. *Paternus, U., 2010. Preoblikovanje vojaških specialnih enot držav zveze NATO. Magistrsko delo, Ljubljana: Fakulteta za družbene vede.*
9. *Prezelj, I., 2007. Nujnost medresorskega sodelovanja in koordiniranja v boju proti terorizmu: nekateri primeri iz Republike Slovenije. V: Bilten Slovenske vojske 2007-9/No. 2. Ljubljana: Generalštab Slovenske vojske, pp. 65–80.*
10. *Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2025 (ReSDPRO SV 2025), 2010. Uradni list R, No. 99/2010 dated 7 December 2010.*
11. *Riper, K. P., 2009. EBO There Was No Baby in the Bathwater. Joint Force Quaterly Issue 52, pp. 82–85.*
12. *Rode, A., 2007. Vojaška obveščevalna dejavnost. Magistrsko delo. Celje: Fakulteta za logistiko.*
13. *Smith, H., 2008. Kinetic and Nonkinetic Versus Lethal and Nonlethal Operations.*
14. *http://www.captainsjournal.com/2008/06/30/kinetic-and-nonkinetic-versus-lethal-and-nonlethal-operations/*
15. *Smith, R., 2006. The Utility of Force. The Art of War in the Modern World. London: Penguin Books.*
16. *Smolej, S., 2011. Kritična analiza na učinku temelječih operacij. Magistrsko delo, Ljubljana: Fakulteta za družbene vede.*
17. *Srednjeročni obrambni program 2007–2012 (SOPR), No. 803-2/2006-58 dated 27 November 2006.*
18. *Spulak, R., 2007. A Theory of Special Operations. Joint Special Operations University (JSOU) Report 07-7. http://jsoupublic.socom.mil/publications/jsou/JSOU07-7spulakATheoryofSpecialOps_final.pdf, 4 June 2010.*
19. *Svete, U., 2007. Asimetrični konflikti in mirovne operacije. Poljče, Center za obrambno usposabljanje. 19 November 2007.*
20. *Svete, U., Guštin, D., Črnčec, D., 2011. Asimetrija in nacionalna varnost: od zgodovinskih izkušenj do sodobnih izzivov. Knjižnica Jurija Vege. Ljubljana: Defensor.*
21. *Vego, N. M., 2006. Effects-Based Operations: A Critique. Joint Force Quaterly Issue 41, pp. 51–75.*

Zoltán Jobbágy
László Szegő

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.6

Pregledni znanstveni članek

RAZPRAVA O ZNAČAJU CILJNO USMERJENEGA NAČRTOVANJA: KRITIKA

DISCUSSING THE NATURE OF OBJECTIVES-BASED PLANNING: A CRITIQUE

Review paper

Povzetek Na proces oblikovanja strategije, kot ga dojema večina zahodnih vojsk, je močno vplival Clausewitz, ki je politični namen razlagal kot končni cilj vojne. Ne glede na vse njegove zasluge in prispevek k teoriji vojne pa se zdi takšen pogled na nastajanje strategije preozek za vojaško delovanje, ki smo mu bili priča v Iraku in še vedno tudi v Afganistanu. V protiuporniškem delovanju vplivajo na postavljanje političnih ciljev in uporabo vojaških sredstev številni dejavniki, tako da oblikovanje strategije pogosto vzbuja videz neurejenega in težavnega procesa, ki temelji na poskusih in napakah. V članku avtorja podrobno osvetlita temo in predstavita svojo kritiko vsesplošnega ciljno usmerjenega pristopa k oblikovanju strategije.

Ključne besede ***Vzročnost, strategija, načrtovanje, napovedovanje, formalizacija.***

Abstract The process of strategy development as seen by most Western militaries is very much shaped by Clausewitz, who regarded the political aim the ultimate goal of war. Despite all his merits and contribution to the theory of war, Clausewitz's approach to strategy development appears to be too narrow for the military engagements we saw in Iraq and still see in Afghanistan. In counter-insurgency operations both the formulation of political goals and the application of military means are influenced by so many factors that strategy development often appears as a messy and painful process of trial-and-error. The authors expand on this issue and deliver a critique to the wide spread objective-based approach to developing strategy.

Key words ***Causality, strategy, planning, prediction, formalisation.***

Introduction

For the last two centuries armed forces have been trained and conditioned to realise predefined objectives at every stage and every level of war. This approach to strategy development can greatly be attributed to Clausewitz, for whom strategy meant nothing more than *"the use of an engagement for the purpose of the war"* (Clausewitz, 1993, p. 207). This rather rational, causal construct, with a clear and concise link between military means and political end, did not hinder him in emphasising that in strategy *"everything [had] to be guessed at and presumed"* (Clausewitz, 1993, p. 211). For Clausewitz, strategy meant a unifying structure to the entire military activity that decided on the time, place and forces with which the battle had to be fought. Consequently, even in Clausewitz causal construct, strategy meant *"numerous possibilities, each of which [would] have a different effect on the outcome of the engagement."* (Clausewitz, 1993, p. 228). The sheer number of possibilities explains why he equated strategy with surprise and argued that *"no human characteristic appears so suited to the task of directing and inspiring strategy as the gift of cunning."* (Clausewitz, 1993, p. 238).

Although Clausewitz regarded the political aim the ultimate goal (end, effect) of war, he equally argued that the multitude of conditions and considerations prohibits its realisation through a single act. As a result, the political end must be decomposed into military means of different importance and purpose. This instrumental focus explains his conviction that *"only great tactical successes [could] lead to great strategic ones"* and his claim that, in strategy, *"there [was] no such thing as victory"*. (Clausewitz, 1993, p. 270, p. 434). Political results at the strategic level mostly come from victories fought at the military tactical level. More politics at the strategic level hence leads to the ability to exploit military victories gained at the tactical level. This was the very reason for him as soldier to claim that in strategy *"the significance of an engagement is what really matters"* (Clausewitz, 1993, p. 617). Despite all the merits and contribution of Clausewitz to the theory of war, his approach to strategy development appears to be too narrow for today's military engagements, such as those seen in Iraq and Afghanistan.

His strong influence on Western military schools of thought resulted in the common understanding of strategy as a link between military means and political ends or, in a more generalised version, between cause (means) and its effect (ends). Consequently, strategy is understood as a plan that expresses clear cause-and-effect assumptions. It provides a rationale for those actions that assumedly help realise political goals. Strategy is thus seen as a rational or planning activity in which means are related to ends in a focused and rigid manner despite the fact that, in most cases, strategy might change should new means become available or different ends appear to be preferable (Betts, 2000; Builder, 1989).

No doubt, war is non-linear in nature, which stands for the brake-down of causality and its underlying ends-means rationality. Counter-insurgency operations, which are high on the agenda in Afghanistan, are frustratingly non-linear. Both the formulation of political goals and the application of military and other means are influenced

by the interplay of so many factors that an approach based on rational planning can only have limited utility. In these cases strategy does not resemble similarity with an elegant forced march, but appears as a messy and painful process of trial-and-error. There are dynamic processes in which military means and political ends become confused. The result is that the means employed and the ends achieved cannot always be delineated sufficiently (Mintzberg, McHugh, 1985).

1 STRATEGY AS EQUATION

Despite the clear non-linear character of recent wars the traditional military approach to strategy development can best be described as an engineering one. Strategy is seen as a rigid framework that rests on ends-means calculation in which the emphasis is on how to synchronise between means applied and ends sought. In most cases a clear definition of ends is followed by a proper organisation of available means for which objectives are set, options narrowed and choices made. According to this approach strategy is appraised in terms of ends rather than means and assumes deliberate, rational and goal-attaining entities. Goals are articulated as objectives and come as a result of a general consensus. They are assumed to be ultimate, identified, well-defined, and sufficiently few that make them both manageable and measurable. The focus is on how well those specific and established objectives are achieved at every level of military operations (Feld, 1959; Beinhocker, 1999; Robbins, 1987; Pirnie, Gardiner, 1996).

Clausewitz stated in accordance that *"the subjugation of the enemy is the end, and the destruction of his fighting forces the means."* (Clausewitz, 1993, p. 637). Hence, the essence of this sort of strategy can be pressed into a very simple equation:

Strategy = Ends + Ways + Means

Ends are equivalent to military objectives, ways to military strategic concepts and means to military resources. Strategy focuses on ways in order to employ means to achieve ends. It is a plan of actions in a synchronized and integrated framework that helps achieve various objectives at theatre, national, and/or multinational levels (Dorff, 2001; Lykke, 2001; Department of Defense, 2001).

This approach indicates the military as a self-sufficient system that contains the necessary means both to determine and attain objectives. Planning is seen as a balancing act between the two and supported by the following two assumptions.

1. The enemy opposition is often regarded as something that falls outside the system. It is seen as an environmental peculiarity that can be overcome. The enemy is simply not allowed to affect clear reasoning, drawing up and pursuit of objectives. War is often subdivided into various headings such as strategy, operations and tactics and often, competence in one area does not mean competence in the other.
2. The military is seen as a rational machine in which decisions are governed by prediction and control. A high degree of stability and calm is required in order

to provide a basis for the rational patterns of orders as the total body of available information is analysed and reduced. War is a series of discrete actions in which events come in a visible and serial sequence.

In other words, strict military discipline makes it possible that *"nothing occurring in the course of its execution should in any way affect the determination to carry it out."* (Warden, 1989; Wylie, 1967; Feld, 1959, p. 21). The fundamental design of this approach contains neatly delineated steps with objectives placed at the front end and operational plans at the rear. The process of planning starts normally with setting objectives as quantified goals, followed by the audit stage in which a set of predictions about the future is made. Predictions delineate alternative states for upcoming situations, which are also extended by various checklists. In the subsequent evaluation stage the underlying assumption is that similar to firms that make money by managing money, armed forces can make war by managing war. Several possible strategies are outlined and evaluated in order to select one. The following operationalisation stage gives rise to a whole set of different hierarchies, levels and time perspectives. The overall result is a vertical set of plans containing objectives, allocation of resources, diverse sub-strategies and various action programs. The last stage of scheduling is equivalent to the establishment of a programmed timetable in which objectives drive evaluation in a highly formal way as everything is decomposed into distinct and specified elements. The basic assumption is that once the objectives are assembled strategy as an end-product will result. This approach rests on decomposition and formalisation in which strategy development often resembles similarity with mechanical programming (Mintzberg, Ahlstrand, Lampel 1998; Mintzberg, 1994; Mintzberg, 1990; Cleland, Ireland, 1990).

2 PREDICTION AND FORMALISATION

Due to its linear design this approach promotes inflexibility through clear directions as it attempts to impose stability. Although everything is built around existing categories emphasising a planned, structured and formalised process, it contains two possible pitfalls such as predictability and formalisation:

1. Predictability means that it presupposes a course of events and an environment that can be stabilised and controlled. Although even in war it becomes possible to predict certain repetitive patterns, forecasting any sort of discontinuity is practically impossible. Thus, a quick reaction outside the formalised design is often better than the extrapolation of current trends and hoping for the best.
2. Formalisation concerns a process that often detaches thinking from action, strategy from tactics, and formulation from implementation. It requires hard data in the form of quantifiable measures. Strategy is seen as a semi-exact science in which courses of actions are put into dry numbers. This approach can give room for *"strategising and artistic expressions by talented generals."* (Mintzberg et. al. 1998; Mintzberg, 1994; Robbins, 1987; Beinhocker, 1999; Smalter, Ruggles, 1966; Mintzberg, 1990; Daven, 2004, p. 17).

The result is that strategy is defined by attributes such as *"clarity of objective, explicitness of evaluation, a high degree of comprehensiveness of overview, and [...] quantification of values for mathematical analysis."* (Lindblom, 1959, p. 80). These characteristics are further reinforced by the influx of various scientific tools in the form of operations research techniques that attempt to blend the relative predictability of advanced military technology, modern mathematics and rapid data processing tools. Although such techniques make it possible to estimate the probability of hitting a target with certain confidence, their power soon erodes when facing problems that cannot be easily translated into quantifiable formulas. Aggregating military activities into measurable data is technically possible, but the subsequent re-aggregation of analytic results is often unsatisfactory, even for the analysts themselves. Consequently, it is at odds with the more complex and constantly changing attributes of the effects landscape (Millett, Murray, 1988/89; Mankins, 2006).

3 ROLE OF OBJECTIVES

Objectives can best be described as *"clearly defined, decisive, and attainable goals towards which every military operation should be directed."* (Joint Publication 1-02, 2001, p. 308). The essence of objectives-based planning is that higher-level objectives are decomposed into specific tasks and activities down to the lowest possible level. Thus, objectives, tasks and actions are linked hierarchically from top to bottom and across the width and breadth of operations. Clausewitz emphasised that *"[n]o one starts a war ... without being clear in his mind what he intends to achieve ... and how he intends to conduct it. The former is its political purpose; the latter its operational objective."* (Clausewitz, 1993, p. 700). Objectives-based planning relies on the process of identifying objectives, analysing various courses of actions that ends with a plan. Activities become linked around common elements and, theoretically, everybody can see his or her contribution to the overall effort. Obsolete activities can be filtered out and eliminated, activities and resources elaborated based on substitution and scarcity (Kent, 1983; Smalter, Ruggles 1966; McCrabb, 2002; McCrabb, 2003; Joint Publication 1-02, 2001).

Forces are tasked to achieve objectives, which constitute the backbone against which campaigns are planned, executed and assessed. It is a construct in which *"series of secondary objectives ... serve as means to the attainment of the ultimate goal"* (Clausewitz, 1993, p. 228). Objectives flow from top down in a way that national security objectives form the basis for applying national power in order to secure national goals and interest:

1. National military objectives guide the application of military power in various regions of the world.
2. Campaign objectives on a regional operational level guide the successful prosecution of military campaigns.
3. Military campaigns are again decomposed into operational objectives in order to position and deploy forces.

4. Operational tasks and functions serve to achieve operational objectives (Thaler, Shlapak, 1995; Kent, Simons, 1991).

Strategy has the basic purpose of linking these levels in a coherent and clear framework since achieving a supported objective is partly a statement of supporting objectives. The result is that objectives cascade downwards as strategy at one level becomes objective at a level below. This hierarchy defines weight amongst objectives over time at the level needed to attain a higher level objective in any given situation. Strategy links the hierarchy of objectives and provides the framework for achieving them. At each level objectives and strategies are accompanied by a set of processes and actions defined by various criteria and constraints. This sort of strategy development places a premium on mass information since execution requires that those involved have access to all relevant aspects. Unfortunately, the non-linear nature of war as detailed earlier is mostly inaccurate, untimely and incomplete with key pieces missing or hard facts lacking (Thaler, Shlapak, 1995).

Objectives are well suited to the traditional levels of modern wars in which national security objectives and national military objectives are on the strategic level, expressed in political-military terms and serve as a framework for the conduct of campaigns and major operations on the operational level. Tactical level battles and engagements are fought in order to achieve higher level objectives. Thus objectives at each level are linked to a source or actor within the hierarchy. They proceed from the general towards the particular in a deductive fashion until those actions that help attain higher level objectives are identified. This hierarchical design puts emphasis on vertical relationships despite the fact that although some aspects may be quantifiable, but some more remain uncertain. The broad assumption is that lower-level objectives help attain objectives on a higher level as the output from one objective serves as input for others (Pirnie, Gardiner, 1996).

4 INSURGENTS AND IRREGULAR FORCES

Although objectives-based planning presupposes that objectives are defined in a clean and coherent way, there is always a risk that the hierarchical order breaks down. National military objectives may not be articulated in a sufficiently clear and concise way, which hinders the proper articulation of campaign objectives, which again cannot contribute to coherent operational objectives. The result is that the entire process shifts towards hedging against the worst case, and can eventually end up with completely inappropriate options. A good example for confusion of this kind was the bombing campaign during Operation Allied Force in which the final campaign plan, with its phased and incremental nature, left the planners mostly confused regarding the effect their actions should have on the enemy. Joint Publications 1-02 defines strategy as the *"art and science of developing and employing instruments of national power in a synchronized and integrated fashion to achieve theatre, national, and/or multinational objectives"* (Polumbo, 2000; Joint Publication 1-02, 2001, p. 383).

Fighting insurgents and other irregular forces means asymmetry, which increases the difficulty to identify useful and coherent objectives that can guide military actions. Although an adequate intelligence support infrastructure is a prerequisite for selecting an appropriate strategy, the feedback loop required for planning, execution and assessment can easily break down. The result is that accurate information does not flow rapidly with consequences ranging from superfluous repetition of actions to dangerous negligence (Thaler, Shlapak, 1995; Lindblom, 1959). Despite the supposed neat and streamlined design of objectives it is most likely that absence of clear guidance from higher echelons in the form of objectives will increasingly become the rule not the exception. More often, those who should define objectives will be in great need and may demand to get objectives suggested from below (Brocades Zaalberg, 2006). This may pose a crucial challenge in cases in which national and theatre level objectives are not well defined or there is no clear causal relationship between military options and desired political results. Due to the complexity involved, the relationship between military means and political ends can either be subject to uncertainties or poorly understood (Lindblom, 1959).

The situation decision-makers might face can become so highly variable and change so rapidly that the entire hierarchical design can get out of balance with no definite and well-understood inputs to objectives. The assumed clear policy guidance in the form of objectives can often be ambiguous as various fields may overlap or become contradictory. Furthermore, policy makers often have to juggle numerous values simultaneously without always making their rank order clear (Brocades Zaalberg, 2006).

Consequently, even with this well structured, engineering-oriented, semi-scientific approach, it becomes impossible to express and describe objectives with the required detail. Another problem is that objectives expressed on the highest level tend to be abstract in nature. Although they often rely on direct and clear causality, their relevance soon erodes as we move down the hierarchy. (Thaler, Shlapak, 1995; Pirnie, Gardiner, 1996; Betts, 2000; Richards, 1990).

As a precaution, menus of objectives are often suggested to provide a certain baseline for times when the expected guidance from above is either insufficient or unclear. Instead of thinking in a single and rigid plan it is believed that a spectrum of plans forming a pool of various strategic concepts can provide for useful strategies in the case the situation changes, or fails to proceed as assumed originally. However, waging war stands for a complex optimisation problem; therefore it is very questionable whether it becomes ever possible to establish a sufficient pool of flexible and non-committal objectives that can cover the vast array of emerging possibilities (Wylie, 1967).

Strategy development based on political ends translated into political objectives can best be described as a maximising approach since it attempts to control everything that may happen on the effects landscape. Despite the discrepancy between

the relative rigidity and linear character, and the increasing complexity of situations found in operations world-wide, the temptation to stick to this approach is as strong as ever (Ho How Hoang, 2004; McCrabb, 2001; NATO Strategic Commanders, 2001).

Conclusion

The biggest shortcoming of the objectives-based approach is its limited ability to adapt, which is discouraged as much by the articulation of objectives as by the separation between formulation and implementation. Its very essence is to realise specific objectives as the focus is on realizing rather than adapting them. Focusing on objectives is quantitative since it mostly deals with static states and not the transitions between possible states. It is a step-wise and incremental approach that proceeds hierarchically through the various levels of war, despite the fact that such links can become weak or even disappear as events unfold. Non-linearity stands for dynamic and constantly changing processes, in which events are also influenced by what common wisdom would term external circumstances or luck. It is also mentioned that a comprehensive understanding of objectives is needed, which requires that commanders must look at both above and below their respective levels (Mintzberg, Waters, 1985; Pirnie, Gardiner, 1996; Senglaub, 2001; Chakravarthy, 1997; Lykke, 2001).

However, such demand can easily put commanders under increased pressure and lower overall performance. Objectives-based planning attempts to see the end from the beginning and by going into ever finer detail it reflects linear causality. Unfortunately, war seen as a non-linear phenomenon indicates much messiness. Thus, there are serious limitations for such an approach:

1. By going step-wise through the tactical, operational and strategic levels, objectives-based planning suggests that objectives simply add together and war can be seen as a sum, and not the product of many factors.
2. Instead of creating options and opening up new possibilities by discovering niches, objectives-based planning shuts down or at least limits the chance of exploiting emergent opportunities.
3. In sum, objectives-based planning means that we *"pursue relatively singular strategies and thus occupy only one spot on the landscape"*, but do not employ any mechanism that provides for protection *"when the landscape unexpectedly changes"* (Beinhocker, 1999b, p. 100, 102).

Clausewitz's contribution to strategic thinking is unquestionable. However, his goal-seeking approach excludes a whole range of other aspects such as logistic, social and technological issues, which must be considered as equally important in military operations. However, this focus should not come as a surprise since he believed that every human activity is a rational undertaking and governed by reason, which explains why he understood strategy as an objective-oriented, goal-seeking phenomenon (Howard, 1979; Millett, Murray, 1988/89).

Bibliography

1. *Beinhocker, E. D., 1999a. On the Origins of Strategies. The McKinsey Quarterly. Number 4. p. 167-176.*
2. *Beinhocker, E. D., 1999b. Robust Adaptive Strategies. MIT Sloan Management Review. Spring. p. 95-106.*
3. *Betts, R. K., 2000. Is Strategy an Illusion? International Security. Fall. p. 5-50.*
4. *Brocades Zaalberg, T., 2006. Soldiers and Civil Power, Supporting or Substituting Civil Authorities in Peace Operations During the 1990s. PhD Thesis. Amsterdam: University of Amsterdam Press.*
5. *Builder, C. H., 1989. The Masks of War, American Military Styles and Strategy and Analysis. Rand Corporation Research Study. Baltimore: The John Hopkins University Press.*
6. *Chakravarthy, B., 1997: A New Strategy Framework for Coping with Turbulence. MIT Sloan Management Review. Winter. p. 69-82.*
7. *Clausewitz, C. von, 1983. On War. New York: Everyman's Library.*
8. *Cleland, D. I., Ireland, L. R., 1990. Project Management, Strategic Design and Implementation. New York: McGraw-Hill.*
9. *Daven, C. (Capt.), 2004. Effects-Based Operations: Obstacles and Opportunities. Journal of the Singapore Armed Forces. Volume 30. Number 2. http://mindef.gov.sg/safti/pointer/back/journals/2004/Vol30_2/ 3.htm, 31 August 2004.*
10. *Department of Defense. Joint Publication 1-02, Dictionary of Military and Associated Terms. 12 April 2001 (as amended through 30 November 2004). www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf, 16 March 2005.*
11. *Dorff, R. H., 2001. U.S. Army War College Guide to Strategy. Carlisle: U.S. Army War College. pp. 11-18. http://permanent.access.gpo.gov/ lps11754/00354.pdf, 08 March 2005.*
12. *Feld, M. D., 1959. Information and Authority: The Structure of Military Organization. American Sociological Review. Volume XXIV. p. 15-22*
13. *Ho How Hoang, J. (Lt. Col.), 2004. Effects-Based Operations Equals to "Shock And Awe"? Journal of the Singapore Armed Forces. Volume 30. Number 2. http://www.mindef.gov.sg/safti/pointer/back/journals/2004/ Vol30_2/7.htm, 30 August 2004.*
14. *Howard, M., 1979. The Forgotten Dimensions of Strategy. Foreign Affairs. Summer. p. 975-986.*
15. *Kent, G. A., 1983. Concepts of Operations: A More Coherent Framework for Defense Planning, Santa Monica: RAND N-2026-AF.*
16. *Kent, G. A., Simons, W. E. 1991. A Framework for Enhancing Operational Capabilities, Santa Monica: RAND R-4043-AF.*
17. *Lindblom, C. E., 1959. The Science of "Muddling Through". Public Administration Review. Spring. p. 79-88.*
18. *Lykke, A. F., 2001. U.S. Army War College Guide to Strategy. Carlisle: U.S. Army War College. 2001. pp. 179-186 http://permanent.access.gpo.gov/ lps11754/00354.pdf, 08 March 2005.*
19. *Mankins, M. C., Steele, R., 2006. Stop Making Plans; Start Making Decisions. Harvard Business Review. January. p. 76-84.*
20. *McCrabb Maris "Buster" Dr., 2001. Explaining "Effects": A Theory for an Effects-Based Approach to Planning, Executing and Assessing Operations. http://www.dtic.mil/jointvision/ideas_concepts/ebo.doc, 23 March 2005.*
21. *McCrabb Maris "Buster" Dr., 2002. Concept of Operations for Effects-Based Operations. Air Force Research Laboratory. http://www.eps.gov/EPSdata/ USAF/Synopses/1142/Reference-Number-PRDA-00-06-IKFPA/ LatestEBOCONOPS.doc, 03 March 2003.*
22. *McCrabb, Maris "Buster" Dr., 2003. Uncertainty, Expeditionary Air Force and Effects-Based Operations. Air Force Research Laboratory. http://www.eps.gov/ EPSdata/USAF/Synopses/1142/Reference-Number-PRDA-00-06-IKFPA/ uncertaintyandoperationalart.doc, 23 March 2003.*

23. *Millett, A. R./Murray, W., 1988/89. Lessons of War. The National Institute, Winter p. 83-95*
24. *Mintzberg, H., Ahlstrand B., Lampel J., 1988. Strategy Safary, A Guided Tour Through The Wilds of Strategic Management. New York: The Free Press.*
25. *Mintzberg, H., 1994. The Rise and Fall of Strategic Planning. Harvard Business Review. January-February. p. 107-114.*
26. *Mintzberg, H., 1990. The Design School: Reconsidering the Basic Premises of Strategic Management, Strategic Management Journal. March-April. p. 171-195.*
27. *Mintzberg, H., McHugh, A., 1985. Strategy Formation in an Adhocracy. Administrative Science Quarterly. June. p. 160-197.*
28. *Mintzberg, H., Waters J. A., 1985. Of Strategies, Deliberate and Emergent. Strategic Management Journal. Volume 6. p. 257-272.*
29. *NATO Strategic Commanders. 2003. Strategic Vision: The Military Challenge, MC 324/1 as of 12. 01. 2003. http://www.dmkn.de/1779/ ruestung.nsf/cc/WORR-66SFNQ. 17 January 2005.*
30. *Pirnie, B., Gardiner, S. B., 1996. An Objectives-Based Approach to Military Campaign Analysis, Santa Monica: RAND MR656-JS.*
31. *Polumbo, H. D. (Col.), 2000. Effects-based Air Campaign Planning: The Diplomatic Way to solve Air Power's Role in the 21st Century, Air War College, Air University, Air Force Academy, April, pp. 6-24.*
32. *Richards, D., 1990. Is Strategic Decision Making Chaotic? Behavioral Science. Volume 35. p. 219-232.*
33. *Robbins, S. P., 1987. Organisation Theory: Structure, Design, and Application. New York: Prentice-Hall International Editions.*
34. *Senglaub, M., 2001. Course of Action Analysis within an Effects-Based Operational Context. Sandia Report. Sand2001-3497. November. www.infoserve.sandia.gov/cgi-bin/techlib/access.control.pl/2001/ 013497.pdf. 23 September 2004.*
35. *Smalter, D. J., Ruggles, R. L., 1966. Six Business Lessons from The Pentagon. Harvard Business Review. March-April. p. 64-75.*
36. *Thaler, D. E., Shlapak, D. A., 1995. Perspectives on Theater Air Campaign Planning, Santa Monica: RAND MR-515-AF.*
37. *Warden, J. A. (Col.), 1989. The Air Campaign, Planning for Combat. Washington: National Defence University Press.*
38. *Wylie, J. C., 1967. Military Strategy: A General Theory of Power Control. New Brunswick: Rutgers University Press.*

Avtorji

Authors

Ján Spišák

Ján Spišák, polkovnik v pokoju od 2009, je diplomiral iz inženirstva na Vojaški akademiji za kopenske sile. Med drugim je opravljal dolžnosti poveljnika tankovskega voda, namestnika načelnika štaba v polku, načelnika J-3 v poveljstvu mehanizirane brigade, namestnika načelnika J-3 v poveljstvu mehanizirane divizije in namestnika direktorja Centra za doktrino v Centru za usposabljanje in doktrino Čeških oboroženih sil. Po generalštabnem šolanju je vodil Oddelek za umetnost vojskovanja na Obrambni univerzi. Trenutno predava na Oddelku za vseživljenjsko učenje na Fakulteti za ekonomijo in management, kjer se je specializiral za vojaško strategijo in operatiko.

Ján Spišák, *Col (Ret. 2009), holds an engineers diploma from Ground Forces Military Academy. His past positions included tank platoon commander, regiment deputy chief of staff, chief J3 (Mechanized Brigade HQ), deputy chief J3 (Mechanized Division HQ), deputy director, Doctrine Centre at the Czech Armed Forces Training and Doctrine Centre. After the General Staff Course, he served as Head of Department of Military Art Studies at the University of Defense. He holds lectures at the Department of Lifelong Learning of the Faculty of Economics and Management specializing in military strategy and operational art.*

Uroš Svete

Dr. Uroš Svete je doktor znanosti s področja obramboslovja, proučuje pa tudi nacionalnovarnostne vidike osamosvajanja Slovenije. Od leta 2000 je zaposlen na Katedri za obramboslovje, trenutno je tudi njen predstojnik. Je član svetovne sociološke zveze (ISA), v kateri znotraj raziskovalnega odbora Armed Forces and Conflict Resolution opravlja naloge izvršnega sekretarja.

Uroš Svete *holds a PhD in defence studies and also deals with national security aspects of Slovenia's process of gaining independence. Since 2000, he has been employed at the Defence Studies Chair, currently as Head. He is a member of the International Sociological Association (ISA) and Secretary of its Armed Forces and Conflict Resolution Committee.*

Anja Kolak

Anja Kolak je diplomirala na Katedri za obramboslovje, kjer je pripravila diplomsko nalogo z naslovom Pomen in vloga kriptografije in kriptoanalize na področju zagotavljanja nacionalne varnosti. Od leta 2007 je zaposlena na Fakulteti za družbene vede, od maja 2010 dalje kot raziskovalka na Obramboslovnem raziskovalnem centru. Trenutno sodeluje pri raziskovalnem projektu Preoblikovanje obrambnih politik v sodobnem varnostnem okolju in zaključuje magistrsko delo s področja informacijske varnosti.

Anja Kolak *graduated at the Chair of Defence Studies with a paper entitled »The role and importance of cryptography and cryptanalysis in the provision of national security«. Since 2007, she has worked at the Faculty of Social Sciences and, since 2010, as a researcher at the Defence Research Centre. She currently participates in a research project The transformation of defence policies in contemporary security environment and is soon to complete her master's degree in information security.*

Denis Čaleta

VVU XIV. r. dr. Denis Čaleta je doktor državnih in evropskih študij in docent na Fakulteti za državne in evropske študije. Predava tudi v drugih strokovnih in akademskih okoljih. Področja njegovega raziskovanja so procesi zoperstavljanja terorizmu v nacionalnem in mednarodnem okolju, vloga oboroženih sil v asimetričnem varnostnem okolju, procesi varovanja kritične infrastrukture in tajnosti. Je predsednik Sveta Inštituta za korporativne varnostne študije – ICS Ljubljana, predsednik Slovenskega združenja korporativne varnosti in sodni izvedenec ter cenilec za področje varovanja tajnosti.

Senior uniformed specialist, Class XIV (OF-5) Denis Čaleta, PhD, *earned his PhD degree from the Faculty of National and European Studies. He is professionally and academically active also in other institutions. His research work focuses on national and international counter-terrorism processes, the role of armed forces in an asymmetric security environment, the processes of critical infrastructure protection and information security. He is president of the Institute for Corporative Security Studies – ICS Ljubljana, president of the Slovenian Association of Corporate Security, court expert and information security appraiser.*

Gorazd Rolih

Major Gorazd Rolih je zaposlen kot častnik za zaščito informacij v Sektorju za informatiko in komunikacije na GŠSV. Pri svojem delu se že več let posveča predvsem varnosti informacijskih sistemov in izzivom, ki jih to področje prinaša s seboj. Objavil je nekaj strokovnih člankov v reviji Varnostni forum. Znanje na širokem področju informacijske varnosti želi v prihodnosti nadgrajevati na podiplomskem študiju.

Major Gorazd Rolih *works as Information Security Officer at Information and Communication Division of the SAF General Staff. For several years, he has been focusing his work on security of information systems and related challenges. He has published several professional articles in the Varnostni forum magazine. His wish is to upgrade his information security-related knowledge through post-graduate studies.*

Maja Bolle

Maja Bolle je absolventka magistrskega študija obramboslovja na Fakulteti za družbene vede. V svojem magistrskem delu proučuje varnost odprtokodne programske opreme in njeno vlogo v kibernetičnem bojevanju.

Maja Bolle *is a military science master's study programme candidate at the Faculty of Social Sciences. Her master's thesis focuses on security of the open source software and its role in cyber warfare.*

Anže Rode

Major dr. Anže Rode je diplomiral na Fakulteti za strojništvo in magistriral na Fakulteti za družbene vede Univerze v Ljubljani. V okviru višjega štabnega šolanja na Poveljniško-štabni šoli SV je magistriral na Fakulteti za logistiko Univerze v Mariboru, kjer je tudi doktoriral z doktorsko disertacijo z naslovom Vojaška obveščevalna dejavnost – aktivna obramba pred JRKB/E-terorizmom. V Slovenski vojski je opravljal različne poveljniške in štabne dolžnosti. Leta 2010 je bil poveljnik SVNKON 13 Isafa v Afganistanu. Je poveljnik Enote za specialno delovanje.

Major Anže Rode, PhD, *graduated from the Faculty of Mechanical Engineering and obtained master's degree from the Faculty of Social Sciences, University of Ljubljana. As a student of the SAF Command and Staff School, Senior Staff Programme, he obtained master's degree from the Faculty of Logistics, University of Maribor, and later PhD degree from the same faculty with a paper entitled Military intelligence – active defence against CBRN/E terrorism. He has performed various commanding and staff duties within the SAF. In 2010, he was Commander of SVNCON 13 ISAF in Afghanistan. Currently, he is Commander of the Special Operations Unit.*

Štabni vodnik Kristian Beršnak je diplomant Fakultete za varnostne vede. V Slovenski vojski je zaposlen od leta 1994. Od 1998 je zaposlen v Enoti za specialno delovanje. Med svojim službovanjem se je udeležil dveh mednarodnih operacij in misij. Leta 2004 je v operaciji Isafa opravljal naloge referenta za operativne zadeve S-3 – vodje skupine za zagotovitev delovanja. Leta 2006 je v operaciji NTM-Irak opravljal naloge četnega inštruktorja/svetovalca na Iraški vojaški akademiji.

SFC Kristian Beršnak *graduated at the Faculty of Criminal Justice and Security in Maribor. He has been employed in the Slovenian Armed Forces since 1994. Since 1998, he has been working in the SAF Special Operations Unit. He has been deployed twice, once to operation ISAF as S3 NCOIC in 2004, and once to operation NTM-Iraq as company training instructor/advisor at the Iraqi Military Academy in 2006.*

Stotnik Bojan Langerholc je opravljal različne poveljniške in štabne dolžnosti. Med službovanjem se je udeležil dveh mednarodnih operacij in misij v Čadu in Afganistanu. Višje štabno šolanje je opravil v ZDA. Je namestnik poveljnika Enote za specialno delovanje.

Captain Bojan Langerholc *performed various command and staff duties. He was deployed twice, once to Chad and once to Afghanistan. He completed his Senior Staff Programme studies in the USA. Currently, he is Deputy Commander of the Special Operations Unit.*

Zoltán Jobbágy

Podpolkovnik dr. Zoltán Jobbágy je pripadnik stalne sestave kopenske vojske Madžarskih obrambnih sil. Svojo vojaško kariero je začel leta 1990 kot pehotni častnik. Doktoriral je iz družbenih ved in behaviorizma na Univerzi v Leidenu na Nizozemskem. Področje njegovega raziskovanja vključuje teorijo kompleksnih adaptivnih sistemov, izgube v vojaških operacijah, analogije med vojno in biološko evolucijo ter strateški razvoj dinamičnega spreminjanja okolij.

Lt. Col. Dr. Zoltán Jobbágy *is an active army officer of the Hungarian Defence Forces who started his military career as an infantry officer in 1990. He holds a Ph. D. in Social and Behavioural Science from Leiden University, The Netherlands. His research area is complex adaptive system theory, causality in military operations, analogies between war and biological evolution, and strategy development in dynamic changing environments.*

László Szegő

Brigadir László Szegő je pripadnik stalne sestave letalstva Madžarskih obrambnih sil. Svojo kariero je začel leta 1989 kot letalsko-tehnični častnik. Magistriral je iz varnostnih in obrambnih študij na madžarski Nacionalni obrambni univerzi Zrínyi Miklós, diplomiral pa je tudi na Centru za varnostno politiko v Ženevi. Trenutno je doktorski kandidat na Nacionalni obrambni univerzi Zrínyi Miklós, kjer se pri raziskovanju osredotoča na sodobne, zlasti anglosaksonske strateške teorije.

Brigadier General László Szegő *is an active air force officer of the Hungarian Defence Forces who started his military career as an aviation technical officer in 1989. He holds an MA. in Security and Defence Policy from the Zrínyi Miklós National Defence University and is a graduate of the Geneva Centre for Security Policy. Currently he is a Ph. D. candidate at the Zrínyi Miklós National Defence University with a research focus on contemporary, especially Anglo-Saxon strategic theories.*

Navodila avtorjem za oblikovanje prispevkov

Instructions for the authors of papers

NAVODILA AVTORJEM ZA OBLIKOVANJE PRISPEVKOV ZA SODOBNE VOJAŠKE IZZIVE IN VOJAŠKOŠOLSKI ZBORNIK

Vsebinska navodila

Splošno

Sodobni vojaški izzivi je interdisciplinarna znanstveno-strokovna publikacija, ki objavlja prispevke o aktualnih temah, raziskavah, znanstvenih in strokovnih razpravah, tehničnih ali družboslovnih analizah z varnostnega, obrambnega in vojaškega področja.
Vojaškošolski zbornik je vojaškostrokovna in informativna publikacija, namenjena izobraževanju in obveščanju o dosežkih ter izkušnjah na področju vojaškega izobraževanja, usposabljanja in izpopolnjevanja.

Kaj objavljamo?
Objavljamo prispevke v slovenskem jeziku s povzetki, prevedenimi v angleški jezik, in po odločitvi uredniškega odbora prispevke v angleškem jeziku s povzetki, prevedenimi v slovenski jezik.
Objavljamo prispevke, ki še niso bili objavljeni ali poslani v objavo drugi reviji. Pisec je odgovoren za vse morebitne kršitve avtorskih pravic. Če je bil prispevek že natisnjen drugje, poslan v objavo ali predstavljen na strokovni konferenci, naj to avtor sporočiti uredniku in pridobiti soglasje založnika (če je treba) ter navesti razloge za ponovno objavo.

Tehnična navodila

Omejitve dolžine prispevkov

Prispevki naj obsegajo 16 strani oziroma 30.000 znakov s presledki (avtorska pola), izjemoma najmanj 8 strani oziroma 15.000 znakov ali največ 24 strani oziroma 45.000 znakov.

Recenzije

Prispevki se recenzirajo. Recenzija je anonimna. Glede na oceno recenzentov uredniški odbor ali urednik prispevek sprejme, če je treba, zahteva popravke ali ga zavrne. Pripombe recenzentov avtor vnese v prispevek.
Zaradi anonimnega recenzentskega postopka je treba prvo stran in vsebino oblikovati tako, da identiteta avtorja ni prepoznavna.
Avtor ob naslovu prispevka napiše, v katero kategorijo po njegovem mnenju in glede na klasifikacijo v COBISS spada njegov prispevek. Klasifikacija je dostopna na spletni strani revije in pri odgovornem uredniku. Končno klasifikacijo določi uredniški odbor.

Lektoriranje

Lektoriranje besedil zagotavlja OE, pristojna za založniško dejavnost. Lektorirana besedila se avtorizirajo.

Prevajanje

Prevajanje besedil ali povzetkov zagotavlja OE, pristojna za prevajalsko dejavnost oziroma Šola za tuje jezike PDRIU.

Navajanje avtorjev prispevka

Navajanje avtorjev je skrajno zgoraj, levo poravnano.
Primer:
Ime 1 Priimek 1,
Ime 2 Priimek 2
V opombi pod črto se za slovenske avtorje navede, iz katere ustanove prihajajo. Pri tujih avtorjih je treba navesti tudi ime države.

Naslov prispevka

Navedbi avtorjev sledi naslov prispevka. Črke v naslovu so velike 16 pik, natisnjene krepko, besedilo naslova pa poravnano na sredini.

Povzetek

Prispevku mora biti dodan povzetek, ki obsega največ 1200 znakov (20 vrstic). Povzetek naj na kratko opredeli temo prispevka, predvsem naj povzame rezultate in ugotovitve. Splošne ugotovitve in misli ne spadajo v povzetek, temveč v uvod.

Povzetek v angleščini

Avtorji morajo oddati tudi prevod povzetka v angleščino. Tudi za prevod povzetka velja omejitev do 1200 znakov (20 vrstic).

Ključne besede

Ključne besede (3-5, tudi v angleškem jeziku) naj bodo natisnjene krepko in z obojestransko poravnavo besedila.

Besedilo

Avtorji naj oddajo svoje prispevke na papirju formata A4, s presledkom med vrsticami 1,5 in velikostjo črk 12 pik Arial. Na zgornjem in spodnjem robu naj bo do besedila približno 3 cm, levi rob naj bo širok 2 cm, desni pa 4 cm. Na vsaki strani je tako približno 30 vrstic s približno 62 znaki. Besedilo naj bo obojestransko poravnano, brez umikov na začetku odstavka.

Kratka predstavitev avtorjev

Avtorji morajo pripraviti kratko predstavitev svojega strokovnega oziroma znanstvenega dela. Predstavitev naj ne presega 600 znakov (10 vrstic, 80 besed). Če je avtorjev več, se predstavi vsak posebej, čim bolj zgoščeno. Avtorji naj besedilo umestijo na konec prispevka po navedeni literaturi.

Strukturiranje besedila

Posamezna poglavja v besedilu naj bodo ločena s samostojnimi podnaslovi in ustrezno oštevilčena (členitev največ na 4 ravni).
Primer:
1 Uvod
2 Naslov poglavja (1. raven)
2.1 Podnaslov (2. raven)
2.1.1 Podnaslov (3. raven)
2.1.1.1 Podnaslov (4. raven)

Oblikovanje seznama literature

V seznamu literature je treba po abecednem redu navesti le avtorje, na katere se sklicujete v prispevku, celotna oznaka vira pa mora biti skladna s harvardskim načinom navajanja. Če je avtorjev več, navedemo vse, kot so navedeni na izvirnem delu.
Primeri:

a) knjiga:
Priimek, ime (lahko začetnica imena), letnica. *Naslov dela*. Kraj: Založba.
Na primer:Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press.

b) zbornik:
Samson, C., 1970. Problems of information studies in history. V S. Stone, ur. *Humanities information research*. Sheffield: CRUS, 1980, str./pp. 44–68. Pri posameznih člankih v zbornikih na koncu posameznega vira navedemo strani, na katerih je članek, na primer:

c) članek v reviji
Kolega, N., 2006. Slovenian coast sea flood risk. Acta geographica Slovenica. 46-2, str. 143–167.

Navajanje virov z interneta

Vse reference se začenjajo enako kot pri natisnjenih virih, le da običajnemu delu sledi še podatek o tem, kje na internetu je bil dokument dobljen in kdaj. Podatek o tem, kdaj je bil dokument dobljen, je pomemben zaradi pogostega spreminjanja www okolja.
Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press, str. 45–100. http://www.mors.si/index.php?id=213, 17. 10. 2008.
Pri navajanju zanimivih internetnih naslovov v besedilu (ne gre za navajanje posebnega dokumenta) zadošča navedba naslova (http://www.vpvs.uni-lj.si). Posebna referenca na koncu besedila v tem primeru ni potrebna.

Sklicevanje na vire

Pri sklicevanju na vire med besedilom navedite le priimek prvega avtorja in letnico izdaje. *Primer:* … (Smith, 1997) …
Če dobesedno navajate del besedila, ga ustrezno označite z narekovaji, v oklepaju pa poleg avtorja in letnice navedite stran besedila, iz katerega ste navajali.
Primer: … (Smith, 1997, str. 15) …
Pri povzemanju drugega avtorja napišemo besedilo brez narekovajev, v oklepaju pa napišemo, da gre za povzeto besedilo. *Primer*: (po Smith, 1997, str. 15). Če avtorja navajamo v besedilu, v oklepaju navedemo samo letnico izida in stran (1997, str. 15).

Slike, diagrami in tabele

Slike, diagrami in tabele v prispevku naj bodo v posebej pripravljenih datotekah, ki omogočajo lektorske popravke. V besedilu mora biti jasno označeno mesto, kamor je treba vnesti sliko. Skupna dolžina prispevka ne sme preseči dane omejitve.
Če avtor iz tehničnih razlogov grafičnih dodatkov ne more oddati v elektronski obliki, je izjemoma sprejemljivo, da slike priloži besedilu. Avtor mora v tem primeru na zadnjo stran slike napisati zaporedno številko in naslov, v besedilu pa pustiti dovolj prostora zanjo. Prav tako mora biti besedilo opremljeno z naslovom in številčenjem slike. Diagrami se štejejo kot slike. Vse slike in tabele se številčijo. Številčenje poteka enotno in ni povezano s številčenjem poglavij. Naslov slike je naveden pod sliko, naslov tabele pa nad tabelo.
Navadno je v besedilu navedeno vsaj eno sklicevanje na sliko ali tabelo. Sklic na sliko ali tabelo je: … (slika 5) … (tabela 2) …

Primer slike:

Slika 5: Naslov slike

Primer tabele:

Tabela 2: Naslov tabele

Opombe pod črto

Številčenje opomb pod črto je neodvisno od strukture besedila in se v vsakem prispevku začne s številko 1. Posebej opozarjamo avtorje, da so opombe pod črto namenjene pojasnjevanju misli, zapisanih v besedilu, in ne navajanju literature.

Kratice

Kratice naj bodo dodane v oklepaju, ko se okrajšana beseda prvič uporabi, zato posebnih seznamov kratic ne dodajamo. Za kratico ali izraz v angleškem jeziku napišemo najprej slovensko ustreznico, v oklepaju pa angleški izvirnik in morebitno angleško kratico.

Format zapisa prispevka

Uredniški odbor sprejema prispevke, napisane z urejevalnikom besedil MS Word, izjemoma tudi v besedilnem zapisu (text only).

Naslov avtorja

Prispevkom naj bosta dodana avtorjeva naslov in internetni naslov ali telefonska številka, na katerih bo dosegljiv uredniškemu odboru.

Kako poslati prispevek

Na naslov uredništva ali članov uredniškega odbora je treba poslati tiskano in elektronsko različico prispevka.

Potrjevanje sprejetja prispevka

Uredniški odbor avtorju pisno potrdi prejetje prispevka. Avtorjem, ki sporočijo tudi naslov svoje elektronske pošte, se potrditev pošlje po tej poti.

Korekture Avtor opravi korekture svojega prispevka v treh dneh.

Naslov uredniškega odbora

Ministrstvo za obrambo
Generalštab Slovenske vojske
Sodobni vojaški izzivi
Uredniški odbor
Vojkova cesta 55
1000 Ljubljana
Slovenija
Elektronski naslov
Odgovorna urednica:
liliana.brozic@mors.si

Prispevkov, ki ne bodo urejeni skladno s tem navodilom, uredniški odbor ne bo sprejemal.

INSTRUCTIONS FOR THE AUTHORS OF PAPERS FOR THE CONTEMPORARY MILITARY CHALLENGES AND THE MILITARY EDUCATION JOURNAL

Content-related instructions

General

The Contemporary Military Challenges is an interdisciplinary scientific expert magazine, which publishes papers on current topics, researches, scientific and expert discussions, technical or social sciences analysis from the field of security, defence and the military..
The Military Education Journal is a military professional and informative publication intended for education and informing on achievements and experiences in the field of military education, training and improvement.

What do we publish?
We publish papers in Slovene with abstracts translated into English. If so decided by the Editorial Board, we also publish papers in English with abstracts translated into Slovene.
We publish papers, which have not been previously published or sent to another magazine for publication. The author is held responsible for all possible copyright violations. If the paper has already been printed elsewhere, sent for publication or presented at an expert conference, the author must notify the editor, obtain the publisher's consent (if necessary) and indicate the reasons for republishing.

Technical instructions

Limitations regarding the length of the papers

The papers should consist of 16 typewritten double-spaced pages or 30,000 characters. At a minimum they should have 8 pages or 15,000 characters and at a maximum 24 pages or 45,000 characters.

Reviews

All papers are reviewed. The review is anonymous. With regard to the reviewer's assessment, the Editorial Board or the editor accepts the paper, demands modifications, if necessary, or rejects it. Upon receiving the reviewers' remarks, the author inserts them into the paper.
Due to an anonymous review process, the first page must be designed in the way that the author's identity cannot be recognized.
Next to the title, the author should indicate the category the paper belongs to according to him and according to the classification in the COBISS[1]. The classification is available on the magazine's internet page and at the responsible editor. The Editorial Board determines the final classification.

Proofreading

The organizational unit responsible for publishing provides the proofreading of the papers. The proofread papers have to be approved.

Translating

The translation of the papers or abstracts is provided by the organizational unit competent for translation or the School of Foreign Languages, DDETC.

Indicating the authors of the paper

The authors' name should be written in the upper left corner, aligned left.
Example:
Name 1 Surname 1,
Name 2 Surname 2,
In the footnote, Slovenian authors should indicate the institution they come from. Foreign authors should also indicate the name of the state they come from.

Title of the paper

The title of the paper is written below the listed authors. The font in the title is bold, size 16 points. The text of the title is centrally aligned.

Abstract

The paper should have an abstract of a maximum 1,200 characters (20 lines). The abstract should include a short presentation of the topic, particularly the results and the findings. General findings and reflections do not belong in the abstract, but rather in the introduction.

Abstract in English

The authors must also submit the translation of the abstract into English. The translation of the abstract is likewise limited to a maximum of 1,200 characters (20 lines).

Key words

Key words (3-5 also in the English language) should be bold with a justified text alignment.

Text

The authors should submit their papers on an A4 paper format, with 1.5 line spacing, fontArial size 12 points. At the upper and the bottom edge, there should be approx. 3 cm of space; the left margin should be 2 cm wide and the right margin 4 cm. Each page consists of approx. 30 lines with 62 characters. The text should have a justified alignment, without indents at the beginning of the paragraphs.

[1] *Co-operative Online Bibliographic System and Services*

A brief presentation of the authors

The authors should prepare a brief presentation of their expert or scientific work. The presentation should not exceed 600 characters (10 lines, 80 words). If there are several authors, each should be presented individually, as shortly and as comprehensively as possible. These texts should be placed at the end of the paper, after the cited literature.

Text structuring

Individual chapters should be separated with independent subtitles and adequately numbered.
Example:
1 Introduction
2 Title of the chapter (1st level)
2.1 Subtitle (2nd level)
2.1.1 Subtitle (3rd level)
2.1.1.1 Subtitle (4th level)

Referencing

In the bibliography, only the authors of references one refers to in the paper should be listed, in the alphabetical order. The entire reference has to be in compliance with the Harvard citing style.

Example:
Surname, name (can also be the initial of the name), year. *Title of the work.* Place. Publishing House.

Example:
Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press.

With certain papers published in journals, the author should indicate, at the end of each reference, a page on which the paper can be found.

Example:
Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press. p. 45-100.

Referencing internet sources

All references start the same as the references for the printed sources, only that the usual part is followed by the information about the Internet page on which the document was found as well as the date on which it was found. The information about the time that the document was found on the Internet is important, because the WWW environment changes constantly.
Urlich, W., 1983. *Critical Heuristics of Social Planning*. Chicago: University of Chicago Press. p. 45-100. http://www.mors.si/index.php?id=213, 17 October 2008.
When referencing interesting WWW pages in the text (not citing an individual document) it is enough to state only the Internet address (http://www.vpvs.uni-lj.si). A separate reference at the end of the text is therefore not necessary.

Citing

When citing sources in the text, indicate only the surname of the author and the year of publication. *Example:* ….. (Smith, 1997) …
When making a direct reference to a text, the cited part should be adequately marked with quotation marks and followed by the exact page of the text which the citing is taken from.
Example: ...(Smith, 1997, p.15) …

Figures, diagrams, tables

Figures, diagrams and tables in the paper should be prepared in separate files which allow for proofreading corrections. The place in the text where the picture should be inserted must be clearly indicated. The total length of the paper must not surpass the given limitation.
Should the author not be able to submit the graphical supplements in the electronic form due to technical reasons, it is exceptionally acceptable to enclose the figures to the text. In this case the author must write a sequence number and a title on the back of each picture and leave enough space in the text to include it. The text must likewise contain the title and the sequence number of the figure. Diagrams are considered figures.
All figures and tables are numbered. The numbering is not uniform and not linked with the numbering of the chapters. The title of the figure is stated beneath it and the title of the table is stated above it.
As a rule, the paper should include at least one reference to a figure or a table..
Reference to a figure or a table is: … (Figure 5) …… (Table 2) ……

Example of a figure:

Figure 5: Title of the figure

Example of a table:

Table 2: Title of the table

Footnotes

The numbering of the footnotes is not related to the structure of the text and starts with number 1 in each paper. We want to stress that the aim of the footnotes is to explain the thoughts written in the text and not to reference literature.

Abbreviations

When used for the first time, the abbreviations in the text must be explained in parenthesis; therefore no additional list of abbreviations is needed. If the abbreviations or terms are written in English, the appropriate Slovenian term should be written along with the English original and possibly the English abbreviation in the parenthesis.

Format type of the paper

The Editorial Board accepts only the texts written with a MS Word text editor and only exceptionally those in the 'text only' format.

Author's address Each paper should include the author's address, e-mail or a telephone number, so that the Editorial Board can reach him or her.

Sending the paper A print or an electronic version of the paper should be sent to the address of the Editorial Board or the members of the Editorial Board.

Confirmation of the reception of the paper The Editorial Board sends the author a written confirmation regarding the reception of the paper. The authors who also list their e-mails receive the confirmation via e-mail.

Corrections The author makes corrections to the paper within three days.

Editorial Board address

Ministry of Defence
Slovenian Armed Forces
General Staff
Contemporary Military Challenges
Editorial Board
Vojkova cesta 55
1000 Ljubljana
Slovenia
Electronic address:
Editor in Chief:
liliana.brozic@mors.si

The Editorial Board will not accept papers, which will not be in compliance with the above instructions.

Dodatek

Appendix

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.3.PREV

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 s sistemskim pristopom, 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, CERT1, 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.

[1] *Computer Emergency Response Team.*

In the Republic of Slovenia, it will be necessary to plan measures to counter cyber 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***

Uvod

Globalizacija sveta in s tem posredno globalizacija varnosti postavlja moderno družbo pred zahtevna vprašanja, po eni strani, kako še naprej svoj razvoj utemeljevati na glavnih postulatih prostega pretoka blaga, storitev in ljudi, ter po drugi, kako grožnje obvladovati na sprejemljivi ravni tveganja. Pojav asimetričnih oblik ogrožanja nacionalne in mednarodne varnosti izhaja iz popolnoma drugih predpostavk in dojemanja osnovnih konceptov zagotavljanja varnosti, ki je še nekaj časa po koncu hladne vojne temeljila na statičnem pristopu k obvladovanju 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. Pojav nedržavnih akterjev, ki so vstopili v interakcijo med tradicionalne subjekte mednarodnih odnosov, je na površje potisnil nove oblike varnostnih groženj, ki so asimetrične in se jim s tradicionalnimi sistemi in vzvodi ni bilo več mogoče učinkovito zoperstaviti. Dinamične spremembe in nesluten tehnološki razvoj so tej dimenziji dodali še kompleksnejšo obliko. Dejstvo, da je moderna družba danes v celoti odvisna od delovanja informacijske in komunikacijske tehnologije, to družbo z varnostnega vidika dela še bolj ranljivo, posamezne grožnje nemotenemu delovanju kritične infrastrukture in tveganja zaradi njih pa še bolj neobvladljive[3]. Nekateri deli te infrastrukture so za delovanje družbe tako pomembni, da bi njihovo nedelovanje ali omejeno delovanje lahko povzročilo hude posledice ali težave. To infrastrukturo imenujemo kritična infrastruktura in jo poskušamo definirati tako na nacionalni kot tudi na mednarodni ravni, seveda odvisno od učinkov, ki bi jih imelo njeno nedelovanje ali uničenje.[4] V tem okviru sta po našem mnenju še posebej izpostavljena dva sektorja, in sicer oskrba z električno energijo ter informacijsko-komunikacijska tehnologija, ki sta neločljivo povezani in soodvisno vplivata na delovanje vseh drugih

---

[2] *Computer Emergency Response Team.*

[3] *62 % ameriške kritične infrastrukture je neposredno priključene na internet ali na IP-omrežje (Secure Computing, 2008).*

[4] *»Kritična infrastruktura državnega pomena v RS obsega tiste zmogljivosti in storitve, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo ter imelo resne posledice na nacionalno varnost, gospodarstvo, ključne družbene funkcije, zdravje, varnost in zaščito ter družbeno blaginjo.« (Sklep Vlade RS, št. 80000-2//2010/3, z dne 19. 4. 2010). V okviru EU pa so definicije naslednje: »kritična infrastruktura« pomeni infrastrukturno zmogljivost, sistem ali njun del, ki se nahaja v državah članicah in je bistven za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi, ter katerih okvara ali uničenje bi imelo v državi članici resne posledice zaradi nezmožnosti vzdrževanja teh funkcij,« in »evropska kritična infrastruktura ali EKI pomeni kritično infrastrukturo, ki se nahaja v državah članicah in katere okvara ali uničenje bi imelo resne posledice v vsaj dveh državah članicah. Kaj so resne posledice se oceni skladno z medsektorskimi merili. To vključuje vplive na druge vrste infrastruktur, ki izhajajo iz medsektorskih odvisnosti« (DIREKTIVA SVETA (ES) št. 114/2008 z dne 8. decembra 2008).*

sektorjev kritične infrastrukture. Zaradi navedenega bomo kibernetskim grožnjam v tem prispevku namenili posebno pozornost. Njihovo učinkovito obvladovanje izpolnjuje pomemben pogoj za nemoteno delovanje informacijsko-komunikacijskih sistemov, ki delujejo znotraj kritične infrastrukture.

1 PREGLED LITERATURE IN TEORETIČNA IZHODIŠČA ZA PROUČEVANO VPRAŠANJE

V današnjem svetu lahko ugotovimo, da sta informacijska in komunikacijska tehnologija zaradi ekonomskih, gospodarskih, sociooloških in kulturnih vplivov postali nepogrešljiv del sodobne informacijske družbe. Nemogoče si je namreč predstavljati delovanje družbe brez ustreznega delovanja informacijsko-komunikacijske tehnologije. V kontekstu razumevanja je treba konkretneje definirati pojem te tehnologije. Evropska unija je v to področje uvrstila medmrežje, zagotavljanje fiksnih in mobilnih telekomunikacij, radijsko in satelitsko komunikacijo in oddajnike. (Svete, 2010)

V okvir mogočih vidikov ogrožanja kritične infrastrukture s področja informacijsko-komunikacijske tehnologije lahko uvrstimo naravne grožnje in grožnje, ki jih povzroča človek. Te pa lahko delimo še v namerno in nenamerno ogrožanje. V svojem prispevku se omejujemo na namerno ogrožanje, pri katerem ima pomembno vlogo teroristično ogrožanje. Zlasti po terorističnih napadih v ZDA leta 2001 se je med varnostnimi strokovnjaki okrepilo mnenje, da bodo informacijski sistemi ena izmed naslednjih tarč teroristov (informacijski terorizem – Cyberterrorism). (Weimann, 2006) Vse večja kompleksnost informacijskih sistemov je varnostni izziv za razvijalce in uporabnike. Analiza trenutnega dogajanja na področju kibernetskih groženj je pokazala, da kibernetski terorizem ni največja grožnja. Protiteroristični koordinator EU meni, da so trenutno na tem področju največja grožnja različna kriminalna omrežja in posamezniki, ki jih podpirajo ali sponzorirajo posamezne države (De Kerchove, 2010).

Lukman in Bernik (2010, str. 5) ugotavljata, da je popolno klasifikacijo kibernetskih groženj težko izdelati, ker se nenehno porajajo nove oblike napadov, ki jih ni mogoče razvrstiti v znane podskupine. Chakrabarti in Manimaran podajata taksonomijo napadov na infrastrukturo interneta kot odgovor na prejšnje razvrstitve, ki so bile usmerjene predvsem v varovanje in zaščito informacij. Napade sta razdelila v štiri osnovne kategorije: napadi na sisteme, prenosne zmogljivosti in programske pakete ter onemogočanje storitev (Chakrabarti, Manimaran, 2003). Za zagotovitev zaupnosti in integritete elektronskih sporočil so bili razviti številni kriptografski algoritmi, ki pa imajo varnostne vrzeli, ki jih izkoriščajo tako sistemski administratorji kot tudi napadalci, da bi izluščili občutljive informacije iz šifriranega omrežnega prometa (Kjaerland, 2005). Razvoj telekomunikacijske infrastrukture poteka tako, da se tradicionalni telefonski sistem in informacijska tehnologija vse bolj združujeta v enotno platformo. Vse hitrejša širitev brezžičnih komunikacijskih sistemov zelo

povečuje možnosti zlorab. V tem primeru namreč tradicionalni obrambni pristop do tveganj, povezanih s kibernetskim prostorom, virtualnim svetom ter terorizmom, dobi kompleksnejšo dimenzijo. Collin virtualni svet opredeljuje kot »/.../ kraj, kjer računalniški programi delujejo in se podatki premikajo.« (v Politt, 1997) Načrtovanje informacijske zaščite teh sistemov zahteva celovit pristop in natančno izvajanje vseh postopkov. Za lažje prepoznavanje vdorov v sisteme so razvili programsko opremo za njihovo odkrivanje in alarmiranje. Kljub visoki tehnični ravni postane programska oprema resnično učinkovita šele v povezavi z analizo. V tem kontekstu ponovno ugotovimo pomen človeškega potenciala in njegovo vlogo v celovitem sistemu zaznavanja obravnavanih groženj. Tun in Aung sta proučila delo analitikov in predlagala orodje za vizualizacijo vdorov (Tun in Aung, 2008). Sisteme za javljanje vdorov je proučeval tudi Kumar, ki predlaga model za avtomatsko klasifikacijo zaznanih vdorov (Kumar, 1994). Kljub številnim razvrstitvam kibernetskih napadov pa lahko vse napade na sisteme kritične infrastrukture razdelimo v tri glavne skupine: vdori v sisteme, onemogočanje storitev ter napadi prek škodljive programske opreme (malware) (Lukman, Bernik, 2010).

Terorizem je v razmerju do uporabe svetovnega spleta povezan na več načinov, in sicer ga uporabljajo kot medij za prenos svojih sporočil ali kot orodje za napad na posamezne cilje. Svetovni splet je postal forum mednarodnega terorizma za širjenje ideologije in novačenje ter mobilizacijo novih članov, zbiranje finančne in materialne podpore, za širjenje sporočil z vsebino sovraštva in nasilja, iskanje informacij, psihološko bojevanje, načrtovanje in usklajevanje dejavnosti ter za medsebojno komunikacijo. Po drugi strani pa poskušajo posamezniki napasti[5] računalniška omrežja, vključno s tistimi, ki so priključena na svetovni splet. (Weimann, 2006)

2 METODE

Analiza mehanizmov zoperstavljanja kibernetskim grožnjam, ki bo opravljena v prispevku, temelji na predpostavki, da se lahko tako kompleksnim grožnjam na nacionalni in mednarodni ravni učinkovito zoperstavimo samo z načrtnimi in ustrezno usklajenimi ukrepi. Analiza daje tisto podlago, s katero nam je omogočeno stvarno ovrednotiti ukrepe, ki jih za zmanjševanje in preprečevanje kibernetskega ogrožanja izvajamo v Republiki Sloveniji. V tem kontekstu v sklepu prispevka podajava tudi posamezne predloge o nujnosti združevanja virov in mehanizmov na področju preprečevanja te grožnje. Ta pristop ima še posebej pomembno vlogo v manjših državah z omejenimi kadrovskimi, finančnimi, organizacijskimi in drugimi viri.

Raziskovalno vprašanje, ki se nam postavlja pri proučevanju mehanizmov odzivanja na kibernetske grožnje, je predvsem, ali so mehanizmi in vzvodi, ki jih ima Republika Slovenija, sposobni ustreznega odzivanja na tako kompleksno grožnjo.

---

[5] *Resnosti groženj z interneta se zavedajo številne države, ki ustanavljajo središča za kibernetsko obrambo (Malezija je ustanovila prvo mednarodno zavezništvo za zaščito pred kibernetskimi napadi, IMPACT – International Multilateral Partnership Against Cyber Terrorism), (Ko, 2008). Nato je v Estoniji ustanovil center odličnosti za kibernetsko obrambo (Cyber Defence Centre of Excellence) (www.nato.int).*

Pri raziskavi tega raziskovalnega vprašanja bomo uporabili tudi več kazalnikov, ki kažejo na podporo političnih struktur vlogi subjektov nacionalnovarnostnega sistema in jih na splošno lahko omejimo na naslednje: (1) število sprejetih zakonskih predpisov, (2) število pripravljenih zakonskih predpisov, (3) jasnost zakonskih predpisov (število vloženih zahtev za razmejitev pristojnosti), (4) število vloženih pobud za spremembo oziroma dopolnitev veljavnih pravnih aktov, (5) količina proračunskih sredstev, (6) pozitivne izjave podpore vodilnih politikov v državi, (7) prisotnost in pogostost programsko-idejne usmerjenosti ter (8) uveljavitev sprejetih zakonskih rešitev v praksi.

V prispevku bomo zato poskušali priti do ugotovitev na podlagi dosedanjega znanja in izkušenj, predvsem pa z različnimi metodološkimi pristopi. Pri pripravi članka bomo kot glavne metode uporabili metode kvalitativne analize, zgodovinsko primerjalno metodo, opisno metodo in metodo vsebinske analize.

Glavne omejitve prispevka so: (1) široko zasnovana tematika, ki odpira številna vprašanja, na katera kljub uresničitvi naštetih ciljev ni mogoče v celoti odgovoriti; (2) razmere, povezane s kibernetskimi grožnjami, se nenehno spreminjajo. Procesi globalizacije vedno znova odpirajo nove možnosti za pojavljanje različnih oblik ogroženosti ter nas postavljajo v situacijo, da je lahko nekaj, kar smo v prispevku ugotovili danes, jutri že zastarelo; (3) podatki o organizaciji sistemov zoperstavljanja kibernetskim grožnjam so v večini držav označeni s stopnjami tajnosti in njihova raba v raziskovalne namene omejena. Poleg tega se je namreč treba zavedati, da je Republika Slovenija s svojimi viri zelo težko primerljiva z drugimi državami.

3 ANALIZA STANJA

Če želimo oceniti stanje na področju sistemskega pristopa k preprečevanju kibernetskih groženj v Republiki Sloveniji in seveda tudi v obrambnem sistemu, je treba opraviti temeljito analizo pravnih in doktrinarnih dokumentov obravnavanega področja. Glede na ugotovitve, da je informacijsko-komunikacijska tehnologija danes povezana skoraj z vsakim področjem, bo analiza pravne podlage usmerjena tudi na področje varovanja kritične infrastrukture, in sicer v tistem delu, ki je neposredno povezan s kibernetsko varnostjo. Rezultati analize so omejeni predvsem na stanje v Republiki Sloveniji, v povezavi z mednarodnim okoljem, ki ga prikazujemo s sklicevanjem na ukrepe EU in Nata. Sledi pregled nekaterih najpomembnejših dokumentov, povezanih s kibernetskimi grožnjami in zaščito pred njimi, ki so opredeljeni v EU in Natu. V nadaljevanju pa bodo analizirani še dokumenti, sprejeti na nadnacionalni ravni.

3.1 Evropska unija

Kadar govorimo o kibernetskih grožnjah, je ključnega pomena zaščita kritične infrastrukture oziroma zaščita kritične informacijske infrastrukture kot njenega sestavnega in zelo pomembnega ter ranljivega elementa. Decembra 2004 je Svet EU sprejel

Evropski program za varovanje kritične infrastrukture (European Programme for Critical Infrastructure Protection – EPCIP), pozneje pa so potekali še seminarji, na katerih so sodelovali vse članice in industrijska združenja, skupaj s strokovnjaki za informacijsko varnost. Evropska komisija je zatem pripravila Zeleno knjigo o evropskem programu za varovanje kritične infrastrukture. Opredeljenih je bilo 11 področij kritične infrastrukture, to so: energetika, informacijska in komunikacijska tehnologija, preskrba z vodo, preskrba s hrano, zdravstvo, finance, javni in pravni red ter varnost, javna uprava, transport, kemična in jedrska industrija ter vesolje in raziskave, ki jih je komisija pozneje v Direktivi o evropski kritični infrastrukturi št. 114/2008 omejila le na dve področji, in sicer na promet in energetiko. Zelena knjiga o evropskem programu za varovanje kritične infrastrukture (EPCIP) iz leta 2005 prinaša pogled Komisije EU na način organiziranja za zaščito evropske kritične infrastrukture (EKI). Z njo so opredeljeni splošni cilj EPCIP kot zagotovitev zadostne stopnje zaščitnih ukrepov, povezanih s kritično infrastrukturo, zmanjšanje kritičnih točk in vzpostavitev obnovitvenih mehanizmov v EU. Poudarjeni so bili trije vidiki ogrožanja, in sicer pristop z upoštevanjem vseh groženj, pristop s poudarkom predvsem na terorizmu, in pristop, ki je upošteval predvsem teroristično grožnjo. Komisija se je v svojem sporočilu, ki je bilo objavljeno po Zeleni knjigi, zavzela za pristop, ki celovito upošteva vse grožnje. Med načeli EPCIP je določen tudi pristop, ki je usmerjen na posamezne sektorje. Glede na to, da imajo sektorji posebne izkušnje, strokovno znanje in zahteve, povezane z varovanjem kritične infrastrukture, se bo za vsak posamezen sektor oblikoval EPCIP, ki se bo uresničeval na podlagi dogovora. Pot do sprejema direktive je bila v okviru EU vsekakor zelo naporna.[6] Direktiva predstavlja začetek postopnega ugotavljanja in določanja evropske kritične infrastrukture ter uveljavljanja potrebe po izboljšanju njenega varovanja. Od prvotno načrtovanih 11 sektorjev je direktiva po kompromisni rešitvi omejena le na energetski in prometni sektor. Namen je, da se v prihodnje ovrednotita njen učinek in potreba po vključitvi drugih sektorjev. Prednost pri tem naj bi imel sektor informacijskih in komunikacijskih tehnologij (Žel, 2011). Republika Slovenija mora kot članica prenesti v svoj pravni red[7] Direktivo Sveta Evropske unije, št. 114/2008 z 8. decembra 2008, o ugotavljanju in določanju evropske kritične infrastrukture ter presoji potrebe za izboljšanje njene zaščite (v nadaljevanju direktiva). Direktiva določa postopek za ugotavljanje in določanje evropske kritične infrastrukture ter skupni pristop za presojo potrebe po izboljšanju zaščite takšne infrastrukture, da bi s tem prispevali k zaščiti ljudi. Obsega energetski ter prometni sektor, lahko pa se uporabi tudi za druge sektorje, v katerih se bo direktiva izvajala.

---

[6] *Ministri za notranje zadeve so zato na neuradnem sestanku v Luksemburgu leta 2008 podprli zamisel, da se namesto direktive oblikuje samo dokument predsedstva, ki bo predstavljal minimalni skupni imenovalec na tem področju. Maja 2008 je bila sprejeta odločitev, da se vendarle sprejme direktiva, ki pa ji je še vedno nasprotovala Švedska. Zaradi tako zelo različnih mnenj in pristopov ter ozaveščenosti držav na tem področju je bila leta 2008 oblikovana okrnjena direktiva, ki predstavlja začetek urejanja EKI.*

[7] *V 12. členu direktive je določeno, da države članice direktivo uveljavijo oziroma sprejmejo predpise, potrebne za njeno uveljavitev. Direktiva določa tudi rok, in sicer je bilo treba besedila predpisov držav članic in njihovo korelacijo z direktivo posredovati Komisiji Evropske unije najpozneje do 12. januarja 2011.*

Podobno potekajo dejavnosti na področju zaščite kritične infrastrukture tudi v Republiki Sloveniji. Problematiko te zaščite smo začeli proučevati predvsem po letu 2006, ko je bila ustanovljena posebna Medresorska koordinacijska skupina za usklajevanje priprav za zaščito kritične infrastrukture (v nadaljevanju medresorska koordinacijska skupina). Ta skupina je leta 2010 pripravila poseben program, ki je vključeval dejavnosti za uveljavitev direktive. Sestavni del programa je bila tudi opredelitev kritične infrastrukture državnega pomena, kar je ena izmed redkih usklajenih rešitev na tem področju. V medresorski koordinacijski skupini je bil pripravljen osnutek predpisa, ki naj bi zagotovil uveljavitev direktive, obenem pa urejal tudi zaščito kritične infrastrukture državnega pomena. Zaščita naj bi bila urejena zlasti v področnih predpisih.

Prvotni namen medresorske koordinacijske skupine je bil torej pripraviti in Vladi RS predlagati v sprejem predlog predpisa (zakona ali uredbe), ki bo povzel vsebino direktive v celoti, hkrati pa določil podlago za urejanje nacionalne kritične infrastrukture v področnih predpisih. Oblikovana je bila posebna podskupina za pripravo normativnopravnega akta za uveljavitev te direktive. V skupini so sodelovali predstavniki ministrstev za gospodarstvo, promet, za notranje zadeve, za visoko šolstvo, znanost in tehnologijo ter za obrambo, predstavniki Generalštaba Slovenske vojske ter Uprave Republike Slovenije za zaščito in reševanje. Skupina se je srečevala s podobnimi težavami kot EU. Dosežena je bila le uskladitev opredelitve kritične infrastrukture evropskega pomena, vsa preostala vprašanja, med katerimi je ustrezna opredelitev javno-zasebnega partnerstva, pa so ostala odprta in neusklajena.

Ministrstvo za obrambo[8], ki je odgovorno za uveljavitev direktive, se je zato odločilo, da se glede na to, da je rok za njeno uveljavitev v slovenski pravni red potekel že 12. januarja 2011, pripravi le Uredba o evropski kritični infrastrukturi. Dodatno je k taki odločitvi prispeval tudi uradni opomin Evropske komisije, ker nacionalni predpisi za prenos Direktive 2008/114/ES z dne 17. 3. 2011 niso bili notificirani. Pozneje je bila ustrezna uredba tudi sprejeta in tako prenesena v notranji pravni red Republike Slovenije.[9] Usklajevanje aktivnosti oziroma podlag in predpisa, ki naj bi uredil zaščito nacionalne kritične infrastrukture, pa bo potekalo posebej. Težava je predvsem pri določitvi ustreznih, razumnih in primernih meril kritičnosti, ki so ključna za oblikovanje predpisa o zaščiti nacionalne kritične infrastrukture.

3.2 Nato

V zadnjem strateškem konceptu (2010, str. 4), ki je bil sprejet novembra leta 2010 na vrhu v Lizboni, je Nato kibernetske grožnje prepoznal kot zelo resne, vse pogostejše, dobro organizirane in vse bolj uničujoče, ne glede na cilj napada (vladne, poslovne,

[8] *To, da Ministrstvo za obrambo vodi koordinacijsko skupino s področja zaščite kritične infrastrukture, je še ena izmed posebnosti Slovenije. V drugih državah je to naloga resorjev, ki se ukvarjajo z notranjimi zadevami, ali posebnih vladnih služb. To si lahko razložimo z dejstvom, da je bilo Ministrstvo za obrambo že prej zadolženo za usmerjanje civilne obrambe, v katero so zdaj vključili tudi kritično infrastrukturo. Drugo dejstvo pa je vsekakor v tem, da si nekateri resorji po spremenjenih razmerah v družbi iščejo novo mesto v sistemu upravljanja posameznih področij nacionalne varnosti.*

[9] *Uradni list RS, št. 35/11.*

ekonomske ali druge organizacije). Potencialno nevarnost vidi Nato v kritični infrastrukturi, če ne bi delovala, bi to lahko prizadelo nacionalne interese in interese zavezništva, blaginjo, varnost in stabilnost. Kot mogoče vire napadov vidi Nato obveščevalne službe, organizirani kriminal ter teroristične in ekstremistične skupine. Nato bo nove trende, povezane z najnovejšo tehnologijo, vključil v svoje procese načrtovanja in prihodnje operacije.

Skladno s strateškim konceptom (2010, str. 5) bo razvijal in uporabljal svoje zmogljivosti za preprečevanje številnih groženj varnosti svojih prebivalcev in obrambo pred njimi. Naštejmo le tiste, ki so povezane z informacijskimi grožnjami:
– sistemi za preprečevanje in zaznavo kibernetskih napadov ter obrambo pred njimi in okrevanje po njih, vključujoč procese načrtovanja za povečanje in usklajevanje nacionalnih zmogljivosti ter centralizirano zaščito, zavedanje, opozarjanje in odzivanje vseh članic;
– razvoj zmogljivosti za zaščito energetskih virov, vključujoč kritično infrastrukturo.

Nato kot legitimno in legalno pravico za zaščito svojih članic omogoča tudi uporabo 5. člena pogodbe[10]. V tem okviru se pojavljajo še nekatera vprašanja, saj je bil člen napisan in sprejet v času, ko informacijskih groženj še nismo poznali, zato v svojem obsegu definira le oborožen napad. Uporaba tega člena v odgovoru na kibernetski napad bi bila tako pravno vprašljiva, tudi če bi bila motiv in napadalec dokazana. Poleg tega se pojavlja tudi vprašanje, kako se ustrezno odzvati na napad. Pri kibernetskem napadu običajno pride do kraje, poneverbe ali izbrisa podatkov, neposredne fizične škode ali človeških žrtev pa ni. Je torej upravičena uporaba sile?

Uporabo 5. člena Severnoatlantske pogodbe zelo intenzivno zagovarja ameriška zunanja politika. Ta meni, da napadi ne bodo več prihajali iz zraka in topov, temveč po optičnih kablih, in da je na kibernetske napade treba odločno odgovoriti, še posebej, če bo tarča napadov kritična infrastruktura (Amies, 2010).

Bruce Schneier (2010) nasprotno meni, da je kibernetski kriminal postal vsakodnevna praksa in da na primer estonski dogodki[11] niso bili nič drugega kot dejanje etnično vznemirjenih ruskih hekerjev zoper protirusko politiko v Estoniji. Hekersko dejavnost sicer obsoja in razume kot resno grožnjo, a opozarja, da je ta v veliki večini delo otrok in objestnežev. Trdi, da je razvijanje ofenzivnih in defenzivnih kibernetskih zmogljivosti povsem legitimno, vendar pa je treba zelo paziti, da ne pride do zlorab. Pri tem izpostavlja ključna problema, kot sta dokazljiv motiv in identifikacija napadalca, ki ju je zelo težko ali celo nemogoče najti oziroma določiti. Kibernetsko vojno označuje za enako verjetno kot konvencionalno in pričakuje hkratno uporabo obeh oblik, če bi do vojne prišlo. Močno zagovarja stališče, da potrebujemo le

---

[10] 5. člen Severnoatlantske pogodbe v glavnem obsega zamisel, ki pravi, da bo oborožen napad na eno izmed članic razumljen kot napad na vse.

[11] Estonija je bila aprila 2007 tarča napadov, domnevno ruskih hekerjev, ki so z DDoS-napadi (DDoS -– denial-of-service je računalniški napad, izveden z velikim številom lažnih zahtev za dostop, ki onesposobijo ciljne računalnike) onemogočili vitalne strežnike in tako začasno skoraj povsem onesposobili delovanje estonskega bančnega sistema in vlade (Layden, 2007).

'mirnodobno' informacijsko varnost, ki temelji na sinergičnem učinku množice zasebnih in javnih organizacij, ki so nam danes že na voljo.

Prvi korak k postavitvi skupnih zmogljivosti za boj proti kibernetskim grožnjam je Nato naredil z ustanovitvijo centra odličnosti v Estoniji (Cooperative Cyber Defence Centre of Excellence – CCDCOE). Center, ki ni del poveljniške strukture Nata, je bil akreditiran 28. 10. 2008 v Talinu (Estonija) in ga financirajo države ustanoviteljice ter sponzorji. Center se ne ukvarja z informacijskimi incidenti, to je naloga NCIRC. Naloge CCDCOE so:
- krepiti in širiti ozaveščenost o informacijskih grožnjah med članicami Nata in partnericami, in sicer z organizacijo izobraževanj, raziskavami in razvojem ter zagotovitvijo informacij in podpore v procesu učenja iz izkušenj (Lessons Learned);
- podpirati Nato pri iskanju dobrih praks, tokov, konceptov in strategij ter pravne podlage za izvajanje operacij informacijskega bojevanja;
- na taktični ravni zagotavljati tehnične rešitve, varnost sistemov v taktičnih okoljih, prepoznavanje informacijskih groženj in napadov ter sanacijo po vdorih, nadzor sistemov, razvoj interoperabilnosti;
- zaščita kritičnih sistemov;
- razvoj metodologije ocene tveganja in varnosti;
- razvoj tehnik modeliranja in simulacij, povezanih z informacijskimi grožnjami (NATO Cooperative Cyber Defence Centre of Excellence, 2011).

3.3 Nacionalna raven

V nadaljevanju bomo prikazali in analizirali strateške dokumente in organe na nacionalni ravni, ki vsebujejo določila, povezana s prepoznavanjem in preprečevanjem pojava kibernetskih groženj in odzivanjem nanje oziroma so bila ustanovljena za ta namen.

Strategija nacionalne varnosti

Vlade nekaterih držav[12] so se po številnih dogodkih, povezanih z informacijskimi incidenti, začele zavedati naraščanja in resnosti teh pojavov. Republika Slovenija je v svoji Resoluciji o strategiji nacionalne varnosti (ReSNV-1), ki začela veljati marca 2010, med vire tveganja nacionalni varnosti uvrstila terorizem, nedovoljene dejavnosti na področju konvencionalnega orožja in orožja za množično uničevanje ter jedrske tehnologije, organizirani kriminal, nezakonite migracije ter seveda tudi kibernetske grožnje. V dokumentu je zapisano: »Zaradi razvejanosti informacijskih in komunikacijskih sistemov, neomejenosti kibernetskega prostora in težav pri nadzoru nad tem prostorom lahko tudi v Republiki Sloveniji pričakujemo širitev različnih oblik računalniške kriminalitete, zlasti kibernetskih vdorov ter napadov državnih in nedržavnih subjektov, ki jih prostorsko in časovno ne bo mogoče omejiti.« (ReSNV-1, 2010, str. 7) Resolucija prepoznava grožnje asimetrične narave kot vse

[12] *V britanski strategiji nacionalne varnosti (National Security Strategy – NSS), ki je bila izdana oktobra 2010, je britanski Svet za nacionalno varnost postavil kibernetske napade in kibernetski kriminal na visoko drugo mesto v prvi skupini tveganj (NSS, 2010, str. 27).*

bolj verjetne, k bojiščem prihodnosti pa poleg kopnega, morja in zraka prišteva tudi kibernetsko okolje. Kot odziv na kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov je v dokumentu zapisano: »Republika Slovenija bo na področju kibernetske varnosti izdelala nacionalno strategijo za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij ter sprejela potrebne ukrepe za zagotovitev učinkovite kibernetske obrambe, v katero bosta v največji možni meri vključena javni in zasebni sektor. Ena od prednostnih nalog na področju zagotavljanja kibernetske varnosti bo tudi ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost.« (ReSNV-1, 2010, str. 16) V teh strateških dokumentih pa manjkajo odgovori, kako v prihodnosti rešiti bistveno vprašanje javno-zasebnega partnerstva, ki je ključno za učinkovito preprečevanje kibernetskega ogrožanja informacijsko-komunikacijske kritične infrastrukture in odzivanje nanj.

Ločnica med javnim in zasebnim sektorjem v odnosu do odgovornosti na področju zaščite kritične infrastrukture se počasi, a vztrajno briše, tako da odgovornost ni le na posameznem segmentu, temveč je deljena. Nesporno je, da je večina kritične infrastrukture v zasebni lasti. To pomeni, da država sama ni več sposobna zagotavljati celovite varnosti te kritične infrastrukture in je močno odvisna od izmenjave informacij in skupnih ukrepov sodelujočih partnerjev. Dobro opredeljeno javno-zasebno partnerstvo je tisti dejavnik, ki je nujen za zagotovitev uspešne politike varovanja kritične infrastrukture. V tem okviru je nujna celovita vizija, ki bo zagotovila ustrezno strategijo in močno politično zavezanost za dosego želenega stanja. Taka vizija mora biti dosegljiva vsem lastnikom kritične infrastrukture. Vizijo, strategijo in ustrezno stopnjo zavedanja lahko opredelimo kot osnovni temelj za katero koli učinkovito politiko varovanja kritične infrastrukture. (Čaleta, 2011)

CERT[13]

CERT-i so danes osnovno orodje za zaščito kritične infrastrukture. Vse države, ki so priključene na internet, morajo imeti zmogljivosti za učinkovito odzivanje na računalniške incidente. Te zmogljivosti so primaren vir zaščite za državo in njene državljane (Porenta, 2011). V Sloveniji imamo SI-CERT (Slovenian Computer Emergency Response Team), katerega naloge so posredovanje pri internetnih incidentih, usklajevanje dela, obveščanje o varnostnih težavah v računalniških omrežjih v Sloveniji in njihovo reševanje. Je kontaktna točka, ki opravlja posredniško in svetovalno vlogo. Deluje znotraj Arnesa (Akademske in raziskovalne mreže Slovenije), vendar pa, kot nakazuje ime, sprejema le prijave varnostnih incidentov za vsa računalniška omrežja v Sloveniji. Arnes in Ministrstvo za javno upravo (MJU) sta na podlagi sklepa Vlade RS, št. 38600-3/2009/21 z dne 31. 5. 2009, podpisala sporazum o sodelovanju na področju informacijske varnosti. Sporazum določa, da bo Arnesov SI-CERT pomagal pri postavitvi vladnega centra, do takrat pa bo za vse informacijske sisteme javne uprave usklajeval odzive na varnostne incidente. Vladni center

[13] *Prvi CERT je bil ustanovljen leta 1988 v ZDA, ustanovitelj je bil ARPA (Advanced Research Projects Agency), in sicer kot odgovor na prvi večji internetni incident – širjenje prvega črva, pozneje imenovanega kar The Internet Worm. S širitvijo interneta so se začele podobne organizacije pojavljati tudi drugje po svetu (CERT-SI, 2011).*

CERT bo specializiran za omrežje in sisteme v javni upravi, medtem ko bo SI-CERT še naprej nacionalna kontaktna točka (Božič, 2011). CERT je organiziran tudi na MO, podlaga za njegovo delovanje je opredeljena v Navodilu o izvajanju ukrepov ob varnostnih dogodkih in incidentih v KiS MO (št. 007-70/2008-1 z dne 6. 3. 2008). Navodilo predpisuje organizacijske in tehnične ukrepe, s katerimi se zagotavlja odzivanje računalniške odzivne interventne skupine (RIOS – angl. CERT) na varnostne dogodke in incidente v KiS MO.

Zavedati se je namreč treba, da je področje, na katerega vpliva kibernetska varnost, izredno široko, kar se kaže tudi v obsegu zakonskih podlag, ki se posredno ali neposredno dotikajo obravnavanega področja. Tudi Republika Slovenija je zato sprejela zakonske predpise, ki se povezujejo s tem področjem, in sicer zakon o varstvu osebnih podatkov, zakon o dostopu do informacij javnega značaja, zakon o elektronskem poslovanju in elektronskem podpisu, zakon o elektronskih komunikacijah, zakon o tajnih podatkih, uredbo o upravnem poslovanju in druge.

4 ANALIZA STANJA NA OBRAMBNEM PODROČJU

Svet za informacijsko varnost

Svet za informacijsko varnost deluje na Ministrstvu za obrambo. Pomemben del njegovih nalog je trenutno usmerjen k vse večjim naporom Nata, da oblikuje koncept skupne kibernetske obrambe, pri čemer imajo vse članice, vključno z Republiko Slovenijo, enakovredno vlogo. Cilja zavezništva, ki izhajata iz Lizbonske deklaracije, sta nadgradnja komunikacijsko-informacijskih sistemov in doseganje polne zmogljivosti kibernetske obrambe do leta 2012. Vsaka članica mora postaviti aktivno zmogljivost CERT, se zavzemati za izboljšanje varnostne kulture, začeti centralno upravljanje omrežij in sistemov ter opredeliti in postaviti sistem varovanja kritične infrastrukture. Po mnenju večine držav članic je namreč pri oblikovanju koncepta ključni element kritična infrastruktura, ki postaja vse pogostejša tarča napadov z interneta. Nekatere članice so zaradi racionalnejše izkoriščenosti virov izpostavile pomembnost sodelovanja med EU in Natom ter sodelovanje nacionalnih CERT z NCIRC (NATO Computer Incident Response Capability). Članice Nata pri oblikovanju koncepta kibernetske obrambe usklajujejo tri področja, ki naj bi bila vključena v pristojnost usklajene Natove kibernetske obrambe:

1. vsa Natova omrežja, omrežja za podporo operacijam zavezništva in omrežja za podporo delovanju poveljstva in agencij;
2. vsa nacionalna komunikacijska omrežja, ki so ključna za Natove operacije;
3. vsa civilna omrežja članic, ki so ključna za delovanje nacionalne kritične infrastrukture.

Članice so pri obravnavi koncepta dosegle načelno soglasje na prvih dveh področjih, na tretjem pa še ne. Nekatere so namreč zadržane do vključitve tretjega področja v Natov koncept.

Svet za informacijsko varnost je konec aprila 2011 v MO imenoval delovno skupino za uskladitev stališč o kibernetski obrambi pred nacionalno obravnavo. Skupina trenutno, preden gredo predlogi na obravnavo na nacionalni ravni, pripravlja predlog aktivnosti MO pri pripravi in uveljavitvi koncepta kibernetske obrambe. Stališče je usmerjeno k nacionalnim in mednarodnim prizadevanjem, k nadgradnji komunikacijskih in informacijskih sistemov ter postavitvi učinkovite zmogljivosti kibernetske obrambe. Pri tem ministrstvo podpira aktivnosti Nata, EU in posameznih članic za oblikovanje kolektivne in nacionalnih zmogljivosti kibernetske obrambe. Pri oblikovanju koncepta in nacionalne strategije kibernetske obrambe sta medresorsko sodelovanje in sodelovanje v zavezništvu izrednega pomena. Dogovorjeno je bilo, da se smiselno uporabijo rešitve dobrih praks, že uveljavljenih v državah EU in Nata, ki se prilagodijo nacionalnim potrebam Slovenije. Ključno pri tem je varovanje nacionalne kritične infrastrukture, ki pa še ni opredeljena. Ministrstvo za obrambo bo aktivneje sodelovalo z NCIRC, ki zagotavlja zmogljivosti odzivanja na računalniške incidente.

4.1 Mednarodna primerjava na obrambnem področju

Pokazalo se je, da so mehanizmi tako mednarodne kot tudi nacionalne zakonodaje v boju proti globalni informacijski grožnji pogosto neučinkoviti. Razlogi za to bi lahko bili:
- ni celovitega in centraliziranega nadzora nad internetom ter komunikacijskimi in informacijskimi sistemi;
- vse države informacijskih groženj ne obravnavajo enako;
- identifikacija napadalcev je izredno zahtevna ali celo nemogoča;
- napadalčev motiv je težko dokazljiv ali celo nemogoč;
- nove tehnologije so vedno korak pred zakonodajo;
- zakonodaja posameznih držav zunaj njihovih meja nima vedno ustreznega učinka.

Zaenkrat še ni dosežen skupen dogovor o tem, kaj kibernetsko ogrožanje sploh je, kako ga prepoznati, dokazati in sankcionirati. V večini primerov se mednarodna skupnost zaveda resnosti problematike, a univerzalne in skupne rešitve še ni (Bosworth, Kabay, 2002, str. 7). Sledi pregled zmogljivosti za zoperstavljanje kibernetskim grožnjam izbranih držav, ki bo v nadaljevanju omogočil lažje razumevanje stanja in umeščenosti tega področja na obrambnem področju v Republiki Sloveniji. Podatki so pridobljeni iz javno dostopnih virov, ki pa se pri Rusiji in Kitajski med seboj razlikujejo in jih je zato treba upoštevati nekoliko z rezervo.

Ameriška vojska verjetno namenja največ virov, tako človeških kot tudi finančnih, za razvoj zmogljivosti na področju kibernetskega bojevanja. Spomladi leta 2010 je ameriški sekretar za obrambo Robert Gates oznanil začetek delovanja poveljstva posebne enote za računalniško bojevanje v sklopu zračnih sil (U. S. Cyber Command – CYBERCOM). Enota je postala polno operativna pol leta pozneje, poveljuje ji general s tremi zvezdicami Rhett A. Hernandez, kar zgovorno priča o njenem pomenu, štela pa bo kar 21.000 pripadnikov. Pripadnike rekrutirajo iz vrst računalniških strokovnjakov in hekerjev, za morebitne operacije pa se bodo, kot

zatrjujejo, pripravljali le najboljši. Američani veliko pozornosti namenjajo forenzičnim zmogljivostim, saj so mnenja, da je zelo pomemben predvsem pravni vidik. Napadalci bodo zelo verjetno na najrazličnejše načine poskušali zabrisati svoje sledi, zaradi česar jih je treba izslediti in identificirati. Prepričani so tudi, da kibernetska obramba sama po sebi ne deluje in da je treba poleg nje graditi tudi ofenzivne metode kot ključni element verodostojne obrambe. (Miles, 2011)

Nemška zvezna vojska je ustanovila posebno enoto, v kateri bodo delovali tako imenovani *hekerji v uniformah*. Trenutno se enota imenuje Oddelek za operacije na področju informatike in računalniških mrež (Abteilung Informations- und Computernetzwerkoperationen), njihova naloga je uriti se v obrambi in protinapadu proti kibernetskim grožnjam. Zvezna vlada je hkrati nemški Zvezni urad za varnost informacijske tehnologije (Bundesamtes für Sicherheit in der Informationstechnik – BSI) dvignila v agencijo za *kiberobrambo*, s čimer je agenciji na voljo več finančnih in kadrovskih virov ter pooblastil (Mann, 2009).

Rusija je v svojem konceptu nacionalne varnosti iz leta 2000 zaradi povečanega razvoja konceptov kibernetskega vojskovanja drugih držav prepoznala kibernetske grožnje kot grožnje svoji nacionalni varnosti. V dokumentu navaja, da bo kibernetski napad ZDA razumela kot vojaško grožnjo in bo nanj odločno odgovorila, pri čemer si jemlje pravico uporabe jedrskega orožja. Znana ruska univerza Tomsk slovi po tem, da izobražuje vrhunske strokovnjake za kibernetsko bojevanje, žal pa nekateri med njimi svoje znanje ponujajo tudi na hekerskem trgu. Iz Rusije izhaja znano *botnet omrežje Storm*, ki ga je sestavljalo ogromno število računalnikov nič hudega slutečih uporabnikov interneta po vsem svetu. Zlonamerna programska koda, s katero so bili okuženi ti računalniki, sama po sebi ni škodljiva, a na računalnikih čaka na ukaze tistih, ki to mrežo upravljajo (CDCOE, 2010).

Tudi Kitajska uspešno sledi težnjam v svetu in domneva se, da tako kot druge velike sile sama razvija zmogljivosti, podprte z informacijsko tehnologijo. V proces modernizacije in informatizacije kitajske vojske je vključeno tudi usposabljanje vojakov za kibernetsko bojevanje, ki poteka v sodobnih računalniških laboratorijih. Temu razvoju se pridružujejo tudi univerze s proučevanjem kibernetske obrambe in napadov, hekerskih metod ter zlonamerne kode. Posebno pozornost Kitajska namenja *kibernetskemu izvidovanju* ali prisluškovanju internetnemu prometu. Znan je primer, kako je Kitajska uspešno izrabila ranljivost internetnega protokola BGP in za 15 minut preusmerila 18 odstotkov svetovnega internetnega prometa na svoje usmerjevalnike. Kitajci so pred tem objavili, da so uspeli izdelati najbolj zmogljiv računalnik na svetu. S takim strojem bi teoretično lahko analizirali tudi internetni promet, a povezava teh dveh dogodkov ni dokazana (Fritz, 2008). Kitajska doktrina namenja asimetrični obliki delovanja veliko pozornosti. Kitajska je država z največjim številom prebivalstva in ogromnim ozemljem, postopoma pa postaja svetovna velesila tudi v ekonomskem smislu. Pri tem si pomaga z razvojem zmogljivosti ofenzivnega kibernetskega delovanja in izvidovanja, s katerim pridobiva različne obveščevalne podatke in tako krepi ekonomsko in vojaško moč. Številne sledi kibernetskih napadov, med

zadnjimi izredno odmeven napad na strežnike Googla, vodijo na Kitajsko, kar je dober dokaz za to, kako tehnološko razvita je ta dežela danes in kako uspešno sledi razvoju v svetu (Fritz, 2008). Kitajske oblasti medtem priznavajo le, da so izurile enoto, imenovano Modra armada, ki jo sestavlja 30 najboljših računalniških strokovnjakov iz vojaških vrst, z univerz in iz drugega civilnega okolja. Usposobljeni naj bi bili izključno za defenzivno delovanje, za mnoge vlade po svetu pa je novica le potrditev njihovega strahu, da so računalniški sistemi resnično lahko kadar koli tarča kitajskih napadov (McConor, 2011).

4.2 Obrambni sistem Republike Slovenije

V svojih strateških dokumentih (ReSNV-1) je Republika Slovenija med viri tveganja za nacionalno varnost prepoznala tudi kibernetske grožnje in se obvezala, da bo pripravila nacionalno strategijo za odzivanje na te grožnje. V ukrepe za zagotovitev učinkovite kibernetske obrambe bo čim več vključila tudi javni in zasebni sektor, ena izmed prednostnih nalog na področju zagotavljanja kibernetske varnosti pa bo ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost. Slovenija je v svojem strateškem dokumentu Resolucija o splošnem dolgoročnem programu opremljanja in razvoja Slovenske vojske do leta 2025 (ReSDPRO 2025), ki je bil sprejet novembra 2010, spoznala, da bo bojišče prihodnosti poleg kopnega, morja in zraka obsegalo tudi kibernetski prostor in vesolje. Posebno pozornost bo Slovenska vojska namenila razvoju (med drugimi zmogljivostmi) zmogljivosti računalniških in komunikacijskih sistemov za zaščito pred kibernetskimi napadi. Kot multiplikatorje bojne moči bo med drugimi razvila tudi zmogljivosti kibernetskega bojevanja. Uvedena bo varna in prilagodljiva komunikacijska in informacijska omrežna infrastruktura, skladna z zahtevami Natovih zmogljivosti omrežnega delovanja. Uvedeni bodo ukrepi in zmogljivosti za informacijsko varnost, namenjeni preprečevanju nenadzorovanega dostopa in vključevanja v omrežje (povzeto po ReSDPRO, 2010).

Slovenska vojska se je v dokumentu (ReSDPRO 2025) obvezala, da bo v prihodnje posebno pozornost namenila razvoju zmogljivosti računalniških in komunikacijskih sistemov za zaščito pred kibernetskimi napadi ter kot multiplikatorje bojne moči med drugimi razvila tudi zmogljivosti kibernetskega bojevanja. V osnutku srednjeročnega obrambnega programa (SOPR 2011–2016), ki je trenutno še v vladni obravnavi, pa je zapisano le, da se bodo ukrepi kibernetske obrambe v Slovenski vojski izvajali skladno z zavezniki in nacionalno strategijo (SOPR, 2011, str. 9), ki pa je Republika Slovenija še nima.

Skladno z dokumenti Evropske unije, evropskega programa za zaščito kritične infrastrukture, je bilo na nacionalni ravni in tudi na MO sprejetih kar nekaj pravnih aktov. MO je ustanovil svoj RIOS (angl. CERT), ki pa še ni zaživel. Delovna skupina s člani z MO, iz SV ter še z nekaterih drugih ministrstev, v sodelovanju s SI-CERT, ki trenutno sicer predstavlja nacionalno kontaktno točko, a ima le posredniško in svetovalno vlogo, sodeluje pri postavitvi vladnega CERT.

Po estonskih napadih se je na informacijske grožnje začel resneje odzivati tudi Nato. Ustanovil je center odličnosti v Estoniji, v katerem razvija zmogljivosti, ki so in bodo v podporo skupnim naporom za boj proti kibernetskim grožnjam. V zadnjem času zavezništvo intenzivno oblikuje skupen koncept kibernetske obrambe. Članice so pri obravnavi dokumenta dosegle načelno soglasje na prvih dveh področjih, na tretjem pa še ne, saj so nekatere zadržane do vključitve svoje kritične infrastrukture v pristojnost usklajene Natove kibernetske obrambe. Slovenija je ustanovila delovno skupino za pripravo nacionalne strategije kibernetske obrambe, pri čemer bo kot izhodišče uporabila primere dobre prakse. Slovenska vojska je v pripravi nacionalne strategije in koncepta kibernetske obrambe z dvema posameznikoma zgolj prisotna v delovni skupini. Virov za razvoj svojih zmogljivosti pa zaenkrat nima.

Zaradi pomembnih novosti, kot so vključevanje nacionalne kritične infrastrukture v Natov koncept ter izdelava nacionalne strategije kibernetske obrambe in koncepta, bi bilo nujno čim prej ustanoviti nacionalni koordinacijski organ za kibernetsko varnost, k čemur se je Slovenija v Resoluciji o strategiji nacionalne varnosti tudi obvezala. Poleg dejstva, da mora Slovenija prispevati svoj delež k zavezništvu, moramo namreč zaščititi predvsem nacionalni interes, to je zavarovati suverenost in avtonomnost svoje kritične infrastrukture. Ker gre v tem primeru tako za politične kot za strokovne odločitve, bi moral biti po najinem mnenju nacionalni koordinacijski organ sestavljen iz skupine strokovnjakov javnega in zasebnega sektorja ter univerz. Usklajeval bi nacionalne aktivnosti in aktivnosti zavezništva ter EU. Uresničeval bi jih lahko po načelih dobre prakse na estonskem primeru in po zgledu agencij iz drugih večjih držav, na primer Nemčije (Bundesamtes für Sicherheit in der Informationstechnik – BSI). Ključna pri tem bi bila dovolj visoka pooblastila, saj je kritična infrastruktura v domeni več različnih ministrstev. Nacionalni koordinacijski organ za kibernetsko varnost bi zato lahko bil umeščen v organizacijsko strukturo Sveta za nacionalno varnost (SNAV), katerega glavne aktivnosti so povezane z zagotavljanjem nacionalne varnosti.

Slovenska vojska bi v procesih za zagotavljanje kibernetske varnosti morala aktivneje sodelovati, in sicer s predstavniki v nacionalnem koordinacijskem organu in z razvojem svojih zmogljivosti ter znanja, upoštevaje kadrovske razmere, v katerih se je znašla. K uvedbi svojih zmogljivosti kibernetskega bojevanja se je obvezala v ReSDPRO 2025. Razvoj teh zmogljivosti je nujen zaradi tajnih podatkov, ki jih je treba zaščititi, posebne narave dela in množice komunikacijsko-informacijskih sistemov, ki jih ima. Vojska bi po zgledu nekaterih razvitejših vojsk morala sama čim bolj zagotoviti suverenost nad svojimi KiS tudi zato, da bi uveljavila neprekinjen proces poveljevanja in kontrole (PINK). Svoje znanje in veščine bi preverjala z udeležbo na mednarodnih kibernetskih vajah, ki so v zadnjem času vse pogostejše. Omenimo le vsakoletno Natovo vajo kibernetske obrambe in vajo, ki jo letos prvič organizira tudi Evropska agencija za informacijsko in omrežno varnost (European Network and Information Security Agency – ENISA). Pomemben kazalnik intenzivnega odzivanja na kibernetske grožnje je tudi dejstvo, da je Slovenska vojska na vaji Pomlad 2011 v scenarij prvič vključila tudi incidente, povezane s kibernetskimi grožnjami.

Sklep

Morebitni napad iz kibernetskega prostora ni več vprašanje, zanima nas samo, kdaj in kako se bo zgodil, kako smo nanj pripravljeni in kako poguben bo. Da je res tako, pričajo številni zaznani primeri iz bližnje preteklosti, nihče ne ve, koliko jih je ostalo tudi skritih. Dejstvo je, da so ti pojavi vedno pogostejši, bolje organizirani in bolj uničujoči. Že na prvi pogled lahko ugotovimo, da bi uresničitev kibernetskih groženj lahko imela hude posledice, paralizirano bi bilo delovanje ključnih sistemov za normalno delovanje družbe, v najslabšem primeru pa bi povzročila tudi negativne ekonomske učinke ali celo smrtne žrtve.

Sredstva, s katerimi bi morebitni napadalci uresničili svoje grožnje, so nam dobro poznana, pa tudi tehnike in metode uporabe. Vseeno pa dovolj zanesljivega sistema obrambe in zaščite še nimamo. Trenutno vsaka država to rešuje po svoje, v večini primerov so organizirani centri CERT, ki se poskušajo spopadati z izzivi kibernetskih napadov, združujejo se tudi med seboj. Nekatere države, kot so ZDA, Velika Britanija, Nemčija in druge, so kibernetske grožnje v svoje strategije nacionalne varnosti postavile na visoko mesto. Imajo tudi nacionalne centre in agencije, ki usklajujejo dejavnosti na nacionalni ravni, vojske teh držav pa intenzivno uvajajo zmogljivosti, s katerimi se bodo poskušale čim bolj učinkovito spopadati s kibernetskimi izzivi. Zaznati je tudi močno zavedanje pomena povezovanja tako različnih nacionalnih ustanov kot tudi pomena povezovanja in sodelovanja med državami, predvsem na ravni EU in Nata. Slovenska vojska zaradi majhnega števila pripadnikov zmogljivosti za zoperstavljanje kibernetskim grožnjam, kakršne imajo velike države, nima, kljub temu pa poskuša slediti tokovom v svetu. To dosega z izobraževanjem strokovnjakov doma in v tujini ter s povezovanjem s civilnimi ustanovami in univerzami pri razvoju in izobraževanju. Slovenija kot članica Nata aktivno sodeluje pri oblikovanju skupne zavezniške strategije kibernetske obrambe. Pravna podlaga za razvoj zmogljivosti za boj proti kibernetskim grožnjam je v RS opredeljena v doktrinarnih dokumentih na nacionalni ravni (ReSNV-1) in na ravni MO (ReSDPRO 2025). Trenutno potekajo aktivnosti za oblikovanje koncepta kibernetske obrambe in nacionalne strategije, pri katerih ima ključno vlogo zaščita nacionalne kritične infrastrukture, ki pa še ni v celoti opredeljena niti medresorsko usklajena. Sklenjeno je bilo, naj se pri oblikovanju uporabijo načela dobre prakse in podpirajo aktivnosti Nata, EU in posameznih članic. Pomembno je tudi sodelovanje z javnim in zasebnim sektorjem ter izobraževalnimi ustanovami.

Slovenska vojska trenutno nima kadrovskih virov niti koncepta za postavitev zmogljivosti kibernetskega vojskovanja, za kar se je v svojih dokumentih obvezala. Z večino aktivnosti se trenutno ukvarja upravni del MO, Slovenska vojska pa pri tem le delno sodeluje. Zoperstavljanje kibernetskim grožnjam tako trenutno poteka le z ukrepi zaščite in varovanja KiS. Vojskovanje v kibernetskem prostoru je danes dejstvo, ki je z nacionalnovarnostnega vidika za prihodnost bistveno večjega pomena, kot se nam morda v tem trenutku zdi. Slovenska vojska bi morala kibernetsko vojskovanje razumeti kot sestavni del svojega vojskovanja in temu primerno tudi pravočasno načrtovati svoje vire.

Literatura

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.*

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.4.PREV

Maja Bolle

Strokovni članek

INFORMACIJSKA VARNOST IN ODPRTOKODNA PROGRAMSKA OPREMA

INFORMATION SECURITY AND OPEN SOURCE SOFTWARE

Professional article

Povzetek Informacijska varnost je ob vedno večji odvisnosti od računalniških sistemov pomembna tema tudi za javno upravo. Ob vedno večjem številu napadov in drugih posegov v integriteto operacijskih sistemov in drugega programja so se mnoge države odločile za prehod na odprtokodno programsko opremo, ki poleg varčevanja pri nakupu programskih licenc državam omogoča tudi večji nadzor nad to opremo. Nekatere raziskave govorijo v prid varnosti zaprtokodnih sistemov, spet druge priporočajo uporabo odprtokodnih. Podatki kažejo, da ima odprtokodna programska oprema na marsikaterem področju boljše varnostne mehanizme kot zaprtokodna, vendar pa ima tudi svoje omejitve. Zaradi teh mora biti prehod držav na odprtokodno programsko opremo dobro premišljen.

Ključne besede ***Odprta koda, odprtokodna programska oprema, zaprtokodna programska oprema, informacijska varnost.***

Abstract In time of increasing dependence on computer systems, information security emerges as an important issue for public administrations. Many governments have made a transition to open source software; the reason being not just financial, but connected to increasing numbers of operating systems security issues. Having more control over the systems is also key. Some research speaks in favor of proprietary software, other in favor of open source software. Data shows that open source software leads over proprietary software in security mechanisms, although they are not without limitations. That is the reason that states transitioning to open source software adoption must take precaution in doing so.

Key words ***Open source, open source software, proprietary software, information security.***

Uvod

Smo v dobi, ko življenje in predvsem delo brez računalnika nista več mogoči. Prav zato je to tudi čas, ko je v ospredju vprašanje informacijske varnosti. Zaradi vedno večjega števila posegov v integriteto najbolj uporabljenih operacijskih sistemov in drugega programja so številne države našle rešitev v prehodu na odprtokodno programsko opremo. Nekatere to pot še iščejo – med njimi je tudi Slovenija. Večina držav se je za prehod na odprtokodno programsko opremo odločila zaradi finančnih razlogov, ne gre pa zanemariti tudi varnostnih (Kimberly, 2005). V članku skušam čim širše predstaviti vprašanje varnosti odprtokodne programske opreme.

Odprtokodna programska oprema (OKPO) je izraz za programsko opremo, katere izvorna koda je prosto dostopna in jo je mogoče prosto uporabljati, raziskovati njeno delovanje, spreminjati in razširjati njene izvirne kot tudi dopolnjene in spremenjene kopije, v primerjavi z zaprtokodno programsko opremo, pri kateri našteto ni mogoče. Pogoji njene uporabe so napisani v različnih licencah, ki vsebujejo smernice uporabe Open Source Initiative. Najpomembnejša merila so prosto razširjanje, dostop do izvorne kode in dovoljenje za spreminjanje ter integracijo te kode (http://www.opensource.org/). OKPO je v uporabi in se razvija predvsem v državah v razvoju (Kshetri, 2004), ponuja jim cenejšo in varnostno zanesljivejšo alternativo zaprtokodnim sistemom.

1 ZGODOVINA IN FILOZOFIJA ODPRTE KODE

Začetki OKPO segajo v petdeseta leta 20. stoletja. Teza, da so ljudje od nekdaj plačevali za programsko opremo, je napačna. Prvi računalniki so bili izjemno veliki, nezmogljivi glede na današnje standarde, predvsem pa so imeli izjemno slabo programsko opremo. Prvi računalnik, ki je bil na voljo za komercialno uporabo, je bil IBM 701 iz leta 1952, za katerega je moral uporabnik na mesec plačevati 15.000 dolarjev uporabnine. Zaradi visoke cene si ga je lahko privoščilo le Ministrstvo za obrambo ZDA, kjer je dobil vzdevek »obrambni kalkulator«. Poznejša različica je bila 705 iz leta 1953, njena cena je bila 1,6 milijona dolarjev. A bolj kot cena je bila vprašljiva programska oprema teh računalnikov. Uporabniški vmesniki so bili uporabniku neprijazni, pa tudi zmogljivost programske opreme je bila manjša, kot jo je omogočala strojna oprema. Ker je bilo programerjev malo, so se uporabniki začeli združevati in si deliti zamisli in programsko opremo, ki bi bolje izkoristila strojne zmogljivosti ter zadovoljila njihove potrebe. Sčasoma so se ustanovila prva združenja, ki so povezovala takšne zanesenjake – najbolj znano je SHARE iz leta 1955. Proti koncu šestdesetih let se je sistem spremenil. Podjetja, ki so prodajala strojno opremo, so kupcu priložila tudi programsko opremo, ki je bila takrat brezplačna (http://www.computerhistory.org/revolution/mainframe-computers/7/172). Po drugi strani pa se je vedno bolj krepil trg, ki je ponujal plačljivo programsko opremo. Ker so se kupci začeli pritoževati, da ne želijo imeti prednaložene programske opreme, češ da naj ne bi zadovoljevala njihovih potreb in da ustvarja monopol, je ameriško sodišče 17. januarja 1969 v sodbi ZDA proti IBM razsodilo, da prednaložena programska oprema zavira konkurenco na trgu (http://history-of-ibm.co.tv/).

1.1 Nastanek prve odprtokodne programske opreme

1.1.1 Unix

Šele leta 1970 je podjetje DEC na tržišču ponudilo prvi računalnik PDP-11, ki je imel dovolj nizko ceno (11.000 USD), da so ga lahko kupili univerze in raziskovalni inštituti (Weber, 2004). Leta 1969 je Ken Thompson izdelal operacijski sistem na računalniku PDP-7 in ga poimenoval UNICS (Uniplexed information and computing services), pozneje so ga preimenovali v Unix. Unix se je začel širiti po univerzah in raziskovalnih inštitutih. Do leta 1972 je bilo namestitev le deset. Veliko prepoznavnost je doživel, ko sta Ken Thompson in Dennis Ritchie leta 1973 na simpoziju ACM predstavila znanstveni članek na temo Unixa. Po objavi članka je število namestitev skokovito naraslo. Podjetje AT&T, pri katerem je bil Thompson zaposlen, je v Unixu zaslutilo poslovno priložnost in zahtevalo njegovo licenciranje. Prva licenca je bila brezplačna in je uporabnikom dovoljevala še precej svoboščin, vendar AT&T zanjo ni omogočal podpore. V vsaki programski opremi neizbežno prihaja do pojava tako imenovanih hroščev (angl. *bug*), napak v programski kodi, ki vodijo v neželene in nepričakovane izide pri njeni uporabi. Vse to je imelo takojšen vpliv na uporabnike Unixa, ki so se začeli povezovati v skupine, skupaj odpravljati hrošče in Unix izboljševati – tega AT&T s svojo licenco ni predvidel. Vseeno pa je bila koda tako zaprta, da so morale te skupine za dostop do izvorne kode AT&T plačati nekaj sto dolarjev. To je storila tudi raziskovalna skupina BTL, ki je izvorno kodo Unixa prepisala v C-programski jezik, s spremembami v kodi pa omogočila, da je Unix od takrat deloval na kakršni koli strojni opremi in katerem koli računalniku. Prav tako je omogočal, da so uporabniki sami izdelovali gonilnike (angl. *driver*) za tiskalnike in podobno opremo, ki so jo potrebovali pri delu. Do leta 1975 je Unix tekel na več kot petdesetih ustanovah po ZDA (Weber, 2004).

1.1.2 BSD

Pomembno vlogo pri razvoju odprte kode ima kalifornijska univerza Berkeley. Tamkajšnji raziskovalci so leta 1973 pod vodstvom profesorja Boba Fabryja ustanovili oddelek za računalniške znanosti, statistiko in matematiko, na katerem so Unix uporabljali, dopolnjevali in spreminjali. Raziskovalca Bill Joy in Chuck Haley sta razvijala in dopolnjevala Unixovo jedro. Leta 1978 je Joy izdelal več dodatkov za Unix, ki jih je skupaj z jedrom spravil v paket, imenovan Berkeley Software Distribution (BSD), vendar to ni bil samostojni operacijski sistem, temveč distribucija Unixa. BSD je postal zelo priljubljen med študenti in raziskovalci, ti so Unix vedno bolj opuščali in raje uporabljali BSD (Weber, 2004).

Leta 1968 je začel delovati predhodnik današnjega interneta, ARPANET. Sprva je povezoval agencijo ameriškega obrambnega ministrstva DARPA (Defense Advanced Research Projects Agency) in druge raziskovalne ustanove. DARPA je želela prek ARPANET-a komunicirati z drugimi ustanovami, vendar sta bila komunikacija in pošiljanje datotek otežena zaradi nezdružljivosti različnih računalnikov in operacijskih sistemov. Ker bi bilo poenotenje strojne opreme drago, se je DARPA obrnila na razvijalce BSD, da bi razvili programsko opremo, ki bi delovala na vseh strojnih

opremah. Fabry je leta 1979 podpisal pogodbo o razvoju BSD, ki bo deloval po željah DARPE. V ta namen je Univerza Berkeley ustanovila nov oddelek, imenovan CSRG (Computer System Research Group), leta 1981 so za DARPO razvili 4.1 BSD. Naslednja različica, 4.2. iz leta 1983, je vključevala nov protokol TCP/IP za medmrežno komunikacijo, ki ga uporabljamo še danes in je temelj današnjega interneta. Različica 4.2 je bila do takrat najhitreje razširjena, naložena je bila na več kot tisoč računalnikov. Prav internet in protokol TCP/IP sta med glavnimi vzroki, da se je začela distribucija BSD množično širiti po medmrežju. AT&T je medtem vedno bolj zaostroval licenco za Unix in ji s tem višal ceno. Leta 1989 je bila cena licence 250.000 USD, česar si univerze niso več mogle privoščiti in so zato prešle na BSD. Da bi lahko ves operacijski sistem ponudili pod licenco BSD in postali neodvisni od AT&T, so ustvarjalci leta 1981 celotno kodo Unixa zamenjali s svojo (Weber, 2004).

1.1.3 Free Software Fundation

Richard Stallman, ki ga danes poznamo kot ustanovitelja Free Software Foundation, je začel v sedemdesetih letih delati na MIT (Massachusetts Institute of Technology). Delal je na oddelku Artificial Intelligence Lab, kjer so raziskovalci razvijali svojo programsko opremo in njeno varnost preizkušali tako, da so drug drugemu vdirali v računalnike. Zelo kmalu je tudi MIT začel omejevati svobodno nameščanje programske opreme. Stallmanu to ni bilo všeč, vrhunec pa je njegovo nezadovoljstvo doseglo leta 1979, ko je njihov oddelek dobil nove laserske tiskalnike podjetja Xerox. Ker so se v tiskalniku nenehno zatikali papirji, je želel sam popraviti programsko opremo tiskalnika in rešiti težavo, vendar mu podjetje Xerox ni želelo dati izvorne kode. Kmalu zatem je na MIT dal odpoved in ustanovil Free Software Foundation. Cilj te neprofitne ustanove je bil narediti popolnoma brezplačen operacijski sistem, katerega izvorna koda bo na voljo vsem in jo bo mogoče tudi svobodno spreminjati. Operacijski sistem je poimenoval GNU (GNU's Not Unix). Leta 1984 je napisal Manifest GNU, v katerem je razložil pomen besede Free Software. Ta ne pomeni nujno brezplačne programske opreme, temveč prosto programsko opremo: prostost se pri tem nanaša na dostopnost do izvorne kode in možnost njenega spreminjanja (beseda *free* v angleškem jeziku ustvarja semantično zmedo, saj ne razlikuje med brezplačen in svoboden, zato je Stallman rešitev poiskal v španskem izrazu *libre*). (Wynants, 2005) Stallman torej ne nasprotuje temu, da ima programska oprema ceno, s katero se plača programerjevo delo, vendar mora biti v svojem bistvu svobodna. V manifestu je napisal štiri temeljna načela, ki veljajo še danes:

1. svoboda uporabljati program v kateri koli namen (svoboščina št. 0);
2. svoboda proučevati program in ga spremeniti po svoji želji. Pogoj za to je dostop do izvorne kode (svoboščina št. 1);
3. svobodno posredovanje kopij (svoboščina št. 2);
4. svoboda izboljšanja programa in objava izboljšav (ter prilagojenih različic) v korist skupnosti (svoboščina št. 3); pogoj za to je dostop do izvorne kode.

Ker se je Stallman zavedal možnosti izkoriščanja teh temeljnih svoboščin, je licenco še dodelal. Ta je nasprotje copyrightu, imenuje pa se General Public License (GPL). Programska oprema, licencirana pod GPL, nikoli ne more postati lastniška, prav

tako tudi ne spremenjena programska oprema, ki izvira iz prostoprogramske, pa tudi nikakršen del kode programske opreme, licencirane pod GPL, ne sme postati del lastniške kode. Sme se izdati le kombinacija lastniške in proste programske opreme, vendar pod pogojem, da se vse licencira pod GPL (Weber, 2004). GPL-licenca je bila sčasoma dopolnjena (zadnja različica je GPL v3) in je služila kot podlaga drugim, bolj specifičnim licencam (http://www.gnu.org/licenses/licenses.html).

1.1.4 Linux

Svetovno najbolj razširjen odprtokodni operacijski sistem na področju superračunalnikov in strežnikov je Linux, ki ima med superračunalniki 91 odstotkov tržnega deleža, za njim sta Unix s tremi odstotki in Windows z enim odstotkom (http://www.top500.org/stats/list/36/osfam). Največji tržni delež ima tudi na področju strežnikov, kar 70,71 odstotka glede na podatke ankete Security Space 2011 (http://www.securityspace.com/s_survey/data/201104/index.html). Vendar pa ima Linux še vedno najmanjši delež na področju namiznih računalnikov (5,1 odstotka), medtem ko imata Windows 85 odstotkov in Mac OS X 8,3 odstotka tržnega deleža (*http://www.w3schools.com/browsers/browsers_os.asp*).

Linux je nastal leta 1991 pod vodstvom takrat 21-letnega Linusa Torvaldsa. 25. avgusta 1991 je v novičarski skupini *comp.os.minix* najavil namero o razvoju jedra novega operacijskega sistema (angl. *kernel*). 17. septembra je na internetu javno objavil prvo različico Linuxovega jedra operacijskega sistema. Ljudi je javno pozval, naj njegov sistem preizkusijo in ga izboljšajo. Linux je iz dneva v dan dobival več podpornikov in razvijalcev, zato je bila že leta 1994 izdana prva različica 1.0.0. Leta 1996 je bila izdana različica 2.0.0, istega leta pa je Torvalds tudi patentiral blagovno znamko Linux (Weber, 2004). Linux danes teče na praktično vsaki računalniški arhitekturi (namizni računalniki, superračunalniki, strežniki, zapestne ure, igralna konzola Playstation 3 ...) (http://www.Linuxfordevices.com/).

Linux je zgolj jedro operacijskega sistema, zato so razvijalci z vsega sveta zanj razvili še grafični vmesnik, namizja, programe, igrice, gonilnike ... in vse to združili v paket, imenovan distribucija. Distribucije temeljijo na posameznem jedru operacijskega sistema (npr. Linux, BSD ...) in se med seboj razlikujejo po tem, kakšno programsko opremo, namizje in skladišča programske opreme vsebujejo. Najbolj razširjena in priljubljena distribucija Linuxa je Ubuntu, ki naj bi jo, glede na podatke, na namiznih računalnikih uporabljalo več kot 12 milijonov ljudi po vsem svetu (Jose, 2011). Po podatkih DistroWatch je na prvem mestu (http://distrowatch.com/) po številu uporabnikov.

2 VARNOST ODPRTOKODNE PROGRAMSKE OPREME

Varnost je relativna, saj jo vsak posameznik dojema drugače. Podobno je z varnostjo odprto- in zaprtokodnih programskih sistemov. Ali je varnejši tisti sistem, ki ima manj hroščev, ali tisti, ki zelo hitro naredi popravke, oziroma tretji, katerega

ranljivost prizadene manj ljudi? Veliko je raziskav, ki govorijo v prid eni ali drugi rešitvi; večina se osredinja zgolj na enega izmed naštetih vidikov (Laurie, 2006). Moja hipoteza je, da je odprtokodna programska oprema varnejša od zaprtokodne. Problematiko skušam predstaviti v čim širšem kontekstu in na različnih področjih, ki so z informacijsko varnostjo tako ali drugače povezana.

2.1 Veliko število distribucij

Po podatkih Distro Watch (http://distrowatch.com/) je na svetu trenutno 320 distribucij, temelječih na operacijskih sistemih, podobnih Linuxu ali Unixu. Resnično število distribucij je v resnici veliko večje, saj lahko doma vsakdo naredi svojo. Prav veliko število distribucij omogoča, da je verjetnost, da bi bila zlonamerna[1] programska oprema pisana za točno določeno distribucijo, veliko manjša, kot je to pri zaprtokodni programski opremi. V dveh najbolj razširjenih zaprtokodnih operacijskih sistemih niti ne poznamo pojma distribucija, saj vsak posameznik kupi operacijski sistem, ki ga ni v več distribucijah, temveč zgolj v različicah (Apple in njegov Mac OS X z različicami Snow Leopard, Lion ... ter Microsoftov Windows z različicami Windows XP, Vista, 7 ...). Vsaka različica teh zaprtokodnih operacijskih sistemov temelji na drugačnem jedru, s čimer se zmanjša prenosljivost zlonamerne programske opreme med njimi. Vendar pa ima zlonamerna programska oprema, ki je pisana za zaprtokodne sisteme, zaradi majhnega števila različic in monokulturnosti Microsoftovih operacijskih sistemov veliko večjo moč razširjanja, saj se različice spremenijo redkeje, kot je to na odprtokodnih operacijskih sistemih, prav tako je zaradi razlik v kodi manjša verjetnost, da bi zlonamerna programska oprema okužila več distribucij (Espiner, 2006). Z vidika informacijske varnosti je veliko število distribucij, ki je značilno za OKPO, torej prednost.

2.2 Zlonamerna programska oprema

Zlonamerna programska oprema je pisana za točno določen operacijski sistem in njegovo različico, saj se izvorna koda med različicami razlikuje. Razširjenost zlonamerne programske opreme, ki je pisana za zaprtokodne in odprtokodne sisteme, je zelo različna. Do danes poznamo več kot dva milijona primerov zlonamerne programske opreme za operacijske sisteme Windows, 1989 primerov za operacijske sisteme Linux in 48 primerov za Apple Mac OS X (Kalkuhl, 2009). Število primerov zlonamerne programske opreme se je v zadnjih dveh letih zelo povečalo, tako na odprto- kot zaprtokodnih operacijskih sistemih. Zadnja poročila inštituta Kaspersky pravijo, da se je število povečalo predvsem zaradi vedno večje priljubljenosti obeh operacijskih sistemov (http://www.securelist.com/en/analysis/204792161/Kaspersky_Security_Bulletin_Malware_Evolution_2010). Največ »zaslug« za novo število primerov zlonamerne programske opreme na področju operacijskih sistemov Linux ima Googlov Android, ki je mobilni odprtokodni operacijski sistem, temelječ na Linuxovem jedru (Racoma, 2011). Zaradi vedno večje priljubljenosti mobilnih

[1] *Kot zlonamerno razumemo (angl. malware) programsko opremo, ki se želi infiltrirati v računalniški sistem ali ga poškodovati, ne da bi pri tem uporabnik privolil v to (Is a Virus or Malware Infection the Cause of Your Slow Computer?, 2011).*

naprav Android je tudi vedno več zlonamerne programske opreme (Sapronov, 2007). Poročilo prav tako ugotavlja, da je od operacijskih sistemov, podobnih Unixu, najbolj na udaru Linux, ki je tudi najbolj razširjen. Vendar statistike kažejo, da je bil Linux napaden predvsem pri strežnikih, manj pa na področju namizja (Sapronov, 2007; Germain, 2008).

Kljub temu da do danes poznamo 1989 primerov zlonamerne programske opreme za OKPO, je njena življenjska doba zelo kratka in v resnici ne naredi toliko škode, kot je lahko naredi na operacijskem sistemu Windows. Razlog tiči v administratorskem dostopu (super user account – bolj znan kot ROOT, do katerega lahko na Linuxu in drugih Unixu podobnih sistemih dostopamo prek ukaza *sudo* – super user do), ki je v Linuxu, BSD in drugih Unixu podobnih operacijskih sistemih iz varnostnih razlogov samodejno deaktiviran, da ne bi nevešči uporabniki upravljali sistema in ga morebiti pokvarili. (https://help.ubuntu.com/community/RootSudo). V praksi to pomeni, da si določimo geslo, s katerim nam je omogočeno spreminjanje vseh nastavitev v operacijskem sistemu, vključno z nameščanjem in odstranjevanjem programov; brez tega gesla pa v sistemu ne moremo spreminjati skorajda ničesar. Drugače je na operacijskih sistemih Windows. Windows prave blokade administratorskega dostopa z geslom ni poznal vse do različic Vista in 7. Blokada pa še vedno ni tako stroga, saj lahko uporabniki v sistemu spremenijo veliko stvari brez administratorskega dostopa (Schneier, 2006). Applov operacijski sistem Mac OS X temelji na Unixovem jedru, pri katerem je administratorski dostop a priori onemogočen in od uporabnika zahteva geslo, podobno kot Linux, kar je dobra lastnost (http://support.apple.com/kb/ht1528). Če pride do okužbe z zlonamerno programsko opremo na Linuxu, škoda ne bo velika, saj ta oprema ne bo imela administratorskega dostopa za ves sistem, njen učinek bo lokaliziran ali pa ga sploh ne bo (http://librenix.com/?inode=21; Koetzle, 2004). Podobno je bilo ugotovljeno v raziskavi Analysis of the Impact of Open Source Software iz leta 2001 (*cardiffschools.net/QinetiQ_OSS_rep.doc*), v kateri so proučevali vpliv virusov na različne operacijske sisteme: Windows je imel takrat več kot 60.000 virusov, Mac OS X in Linux pa po 40. Čeprav večina virusov, pisanih za Windows, ni naredila velike škode, je več sto virusov povzročilo velikansko škodo. Dve tretjini sta naredili veliko škodo Applovemu Mac OS X sistemu, medtem ko niti eden Linuxovih virusov ni povzročil večje škode oziroma se ni bolj razširil po sistemu (Peeling, 2001). Varnost operacijskih sistemov, podobnih Unixu, lahko kljub temu močno ogrozi tako imenovani korenski komplet (angl. rootkit), ki omogoča prikrit dostop do računalniškega sistema in uporabo administratorskih pravic (Chuvakin, 2003).

Kot vidimo, ni tako pomembno, koliko zlonamerne programske opreme obstaja za nek operacijski sistem, pomembneje je, kako široko in na kakšni ravni lahko prizadene sistem. Microsoft je po zgledu odprtokodnih operacijskih sistemov v različicah Vista in 7 onemogočil administratorski dostop in s tem izboljšal varnost sistema.

2.3 Ali veliko oči res več vidi?

Sistem *veliko oči* (angl. many eyes) je sistem pregleda, s katerim ima (teoretično gledano) vsak uporabnik moč pregleda izvorne kode OKPO – s tem je zmanjšana možnost, da bi OKPO vsebovala zlonamerno kodo, kot so stranska vrata, prek katerih lahko nepooblaščena oseba dobi dostop do sistema.

Zagovorniki OKPO pogosto uporabljajo argument, da sistem *veliko oči* omogoča hitro detekcijo hroščev v kodi. V praksi ni tako, večina uporabnikov danes ni veščih programiranja, izvorne kode ne znajo brati ali v njej prepoznati pomanjkljivosti in morebitnih stranskih vrat. OKPO uporabljajo za vsakodnevna opravila, kot so pisanje besedil, urejanje preglednic, pisanje spletne pošte ... Še vedno pa OKPO omogoča vpogled tistim, ki jih to zanima in so tega sposobni. To je pomembna razlika, saj zaprtokodni sistemi tega ne omogočajo (Laurie, 2006).

V zgodovini je bilo več primerov, da več let niso odkrili ranljivosti, čeprav je OKPO pregledalo več ljudi. Eden zanimivejših primerov so stranska vrata Kena Thompsona, ki je bil razvijalec sistema Unix, v katerega je stranska vrata vnesel sam. Šele po 14 letih je Thompson to razkril. S tem malim eksperimentom je želel pokazati, da se na druge ljudi ne smemo preveč zanašati. Po njegovem mnenju je varna samo tista koda, ki jo napišemo sami (O'Dowd, 2004). Tu se nam poraja vprašanje o človeškem dejavniku. Če je kodo pregledalo veliko ljudi, to še ne pomeni, da je bil pregled tudi dovolj natančen ali da so pregledovalci kompetentni za odkritje vseh ranljivosti.

2.4 Čas za popravek

Čas za popravek je čas med tem, ko zaznamo ranljivost v kodi, in časom, ko se naredi popravek. Ta čas je izjemno pomemben in mora biti čim krajši – dlje kot je ranljivost brez popravka, bolj je varnost sistema ogrožena. Raziskava primerjave varnosti pri operacijskih sistemih Windows in različnih Linuxovih distribucijah (Debian, Red Hat, Mandark) v enem letu je pokazala število zaznanih nevarnosti, čas za izdelavo popravka in število popravljenih nevarnosti (Koetzle, 2004). Windows je za izdelavo popravkov v povprečju potreboval najmanj časa, 25 dni, sledile so mu Linuxove distribucije Red Hat in Debian s 57 dnevi in Mandark z 82 dnevi.

Zgolj ta podatek pa za primerjavo varnosti operacijskih sistemov ne zadostuje: pri Windowsih so našteli največ nevarnosti najvišje stopnje (67 odstotkov vseh nevarnosti), sledil je Red Hat s 56 odstotki nevarnosti enake stopnje. Raziskava je merila tudi čas, ki je potreben, da ponudniki vnesejo popravke v distribucijo. Pri OS Windows je bil ta čas enak kot za izdelavo popravkov, saj distribucij sistemov Windows ni. Debian je v povprečju potreboval zgolj 32 dni, kar je veliko manj od časa, ki ga je potreboval za izdelavo popravkov (57 dni), prav tako Red Hat s 47 dnevi. Debian je bil tako hiter, ker je bil edina proučevana distribucija, ki se posodablja, ne da bi bila potrebna ponovna namestitev celotnega sistema (angl. rolling release). Ko distribucijo enkrat namestimo, je ni treba nikoli več nameščati, saj se ves sistem posodablja

samodejno, skupaj z vsemi nameščenimi programi. Zanimivost se je pokazala tudi pri Microsoftu.

Za varnost ni pomemben samo čas izdelave popravkov, predvsem so pomembni uporabniki, ki si morajo te popravke namestiti. Uporabnike Microsofta je ogrožalo devet ranljivosti najvišje stopnje, vendar večina proučevanih kljub temu popravkov več kot 305 dni ni namestila. To pomeni, da so bili v povprečju ogroženi 305 dni, čepav je Microsoft v povprečju izdelal popravke že po 25 dneh (Koetzle, 2004). Podatek lahko kaže na nižjo računalniško pismenost uporabnikov operacijskega sistema Windows v primerjavi z uporabniki Linuxa.

Če ljudje prek sistema *veliko oči* v OKPO odkrijejo ranljivost, to nemudoma objavijo na posebnih spletnih straneh, forumih ipd. (zelo znana taka stran Linuxove distribucije je Ubuntu Bugs Launchpad – https://bugs.launchpad.net/ubuntu/). Razvijalci OKPO ranljivost nato čim hitreje odpravijo. Seveda obstajajo razlike med razvijalci različnih OKPO. Apache v povprečju izdaja popravke vsak dan, tako da ranljivost redko traja dlje od enega dneva. Ubuntu, ki je najbolj razširjena Linuxova distribucija, popravke izdaja glede na prednostni vrstni red, ki se določi prek Ubuntu Bug Launchpad.

Ponudniki distribucij odprtokodnih operacijskih sistemov navadno malce zaostajajo za razvijalci. Tako na primer profesionalni odprtokodni program za 3D-animacijo Blender (http://www.blender.org/) na svoji spletni strani ponuja različico 2.57, medtem ko uporabniki operacijskega sistema Ubuntu prek programskega središča lahko namestijo različico Blender 2.49. Ponudniki svojih baz torej ne osvežujejo skladno z vsakodnevnim razvojem OKPO. To pomanjkljivost odpravlja *skladišče programske opreme* (angl. repository), ki uporabnikom omogoča, da najnovejšo različico programa namestijo neodvisno od ponudnikov distribucije in v trenutku, ko jo razvijalec objavi. Skladišče programske opreme je bilo narejeno za hitrejše posredovanje najnovejše različice programske opreme ter hitrejšo pridobitev povratne informacije o kakovosti te opreme, ki zelo hitro pride do razvijalca, kar pospeši njen razvoj (Laurie, 2006). Leta 2007 je Ubuntu izdal programsko opremo Personal Package Archive (PPA) z namenom, da bi še pospešili in olajšali distribucijo programske opreme prek skladišč (Humbrey, 2011). Ni nujno, da so vsa skladišča varna, saj si lahko dodamo skladišče, ki vsebuje zlonamerno kodo. Zato je priporočeno, da se dodajajo samo skladišča, ki so preverjena in niso sumljivega porekla.

Zaprtokodna operacijska sistema Windows in Mac OS nimata sistema *veliko oči*, temveč za varnost skrbijo razvijalci obeh sistemov. Vseh ranljivosti ne objavljajo javno, zato tudi ne vemo, kako dolgo smo dovzetni zanje in kakšno je njihovo resnično število.

Kot vidimo, večje število javno objavljenih nevarnosti še ne pomeni bolj ranljivega sistema, temveč preglednejšega. OKPO je s tem v prednosti, saj pri zaprtih sistemih zaradi nepreglednosti sistema ne moremo vedeti za vse varnostne ranljivosti.

2.5 Varnost s preglednostjo ali skrivanjem

Velikokrat slišimo, da skrivanje izvorne kode vodi v večjo varnost, vendar to v resnici ne drži. Že eden prvih kriptologov, Auguste Kerckhoffs, je davnega leta 1883 napisal šest načel dobre kriptografije, kar danes imenujemo Kerckhoffsov zakon; ta pravi, da je dober šifrirni sistem varen, tudi če o njem vemo vse, razen šifrirnega ključa. Kerckhoffs prav tako zavrača načelo, da je varnost mogoče zagotoviti s skrivanjem; ne zahteva, da je šifrirni sistem javen, vendar opozarja, da skrivnost ne zagotavlja večje varnosti, temveč jo celo ogroža (Kovačič, 2006). Skriti sistem lahko ogroža varnost tako, da vsebuje napake, ki bi jih, če bi bil javen, odkrili in popravili. Eden največjih strokovnjakov za informacijsko varnost in kriptolog Bruce Schneier pravi: »Ne spominjam se nobenega kriptografskega sistema, razvitega naskrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake.« (Schneier, 2002) Podobno se je zgodilo z zelo znanim primerom podatkovne baze Borland InterBase, v kateri so leta 2000 odkrili stranska vrata (angl. backdoor) takrat, ko je podjetje propadlo in objavilo izvorno kodo programske opreme, ki je bila pred tem lastniška oziroma zaprta. Programerji so ugotovili, da so bila leta 1994 podatkovni bazi namerno dodana stranska vrata, ki so vse do leta 2001 posamezniku omogočala popoln dostop do vseh podatkov in tudi vrivanje podatkov in vsebin z uporabniškim imenom *politically* in geslom *correct*. Še bolj zaskrbljujoče je, da so podatkovno bazo uporabljale bostonska borza in velike korporacije, kot so Motorola, Nokia in Boeing. Na srečo so odprtokodni programerji zelo hitro naredili popravek, ki je ta stranska vrata zaprl (Poulsen, 2001).

V duhu odprte kode tudi Microsoft danes državam omogoča dostop do izvorne kode pod pogoji, ki so napisani v pogodbi Government Security Program. V njej najdemo približno 60 držav, med njimi tudi države Nata, Kitajsko in rusko tajno službo FSB (Espiner, 2010). Vendar je Microsoft tisti, ki določi, ali bo državi razkril izvorno kodo ali ne. Med državami, ki jim Microsoft ne omogoča vpogleda, najdemo Venezuelo, Kubo in druge države, ki so prešle na odprto kodo v javni upravi. Microsoft naj bi se za razkritje izvorne kode odločil iz komercialnih razlogov. Nekateri strokovnjaki opozarjajo na slabost takšnega sistema. Richard Clayton z univerze Cambridge opozarja, da države tako lažje najdejo varnostne ranljivosti, ki jih lahko izrabijo za napad na druge države, saj podatka o ranljivosti ne objavijo javno, zanjo vedo le znotraj sistema, ki ima dostop do izvorne kode. Government Security Program ima tudi to omejitev, da državam omogoča vpogled v izvorno kodo, ne omogoča pa njenega spreminjanja (http://www.microsoft.com/resources/sharedsource/gsp.mspx).

3 PREHOD DRŽAVNIH JAVNIH UPRAV NA ODPRTO KODO

V zadnjem času je vedno več držav, ki se odločajo za prehod na OKPO. Nekatere prehajajo le delno (npr. v nekaterih vladnih agencijah) in uporabljajo zgolj odprtokodno programje, kot so Libre Office ali Open Office namesto Microsoft Office (to so ZDA, Francija, Nemčija, Češka, Makedonija, Južna Afrika in Filipini). Je pa tudi

vedno več držav, ki so se odločile za popoln prehod na OKPO (Kitajska, Rusija, Brazilija, Venezuela, Pakistan, Kuba, Turčija, Malezija in Španija), kar pomeni, da uporabljajo distribucije operacijskih sistemov Linux ali BSD, skupaj s pripadajočo programsko opremo. Večina držav, ki so se odločile za popoln prehod, je ustvarila svoje državne distribucije operacijskih sistemov, ki vsebujejo točno določeno programsko opremo (tisto, ki jo v specifični javni upravi potrebujejo). Te države so zaradi zagotavljanja večje varnosti naredile svoja skladišča, ki jih posodabljajo njihove državne ustanove, vsebujejo pa programsko opremo, ki je bila razvita posebej za državne ustanove. S tem zagotovijo večjo varnost operacijskih sistemov, saj programsko opremo, ki je v skladiščih, pregledajo in razvijajo države same. Varnost je poleg zmanjšanja stroškov eden glavnih razlogov za prehod državnih javnih uprav na OKPO (Lewis, 2006). Ko so leta 1999 prišla v javnost prva poročila, da naj bi ameriška agencija NSA (National Security Agency) vnesla stranska vrata v vsako kopijo operacijskega sistema Windows 95 (Campbell, 1999), so se države zamislile nad varnostjo in nadzorom pri operacijskih sistemih podjetja Microsoft. Zmotile so jih tudi monokulturne monopolistične tendence Microsofta, ki obvladuje več kot 80 odstotkov tržnega deleža na področju namiznih računalnikov. Zaradi tako velikega tržnega deleža ima zlonamerna programska oprema tudi veliko večje možnosti za širitev in uničenje sistema. Microsoft je poleg tega začel kodo dopolnjevati tako, da je omejevala delovanje na drugih sistemih in s tem države *priklenil* nase (angl. vendor lock-in). To je spodbudilo razmišljanje o alternativnih programskih rešitvah, ki bi državam omogočile večji nadzor nad računalniškimi sistemi in večjo preglednost, večjo neodvisnost od Microsofta in možnost razvoja ter prilagajanja sistema svojim potrebam (Geer, 2003). Mnoge so rešitev videle v OKPO.

Nekaj primerov: v Venezueli so razvili svoj operacijski sistem, imenovan Canaima, ki temelji na distribuciji Debian Linux. Državni dekret številka 3390 (http://asl.mct.gob.ve/images/Marco_legal/decreto3390.pdf) veleva uporabo Canaime v javni upravi, prav tako mora biti vsaka posebej razvita programska oprema za javno upravo licencirana pod licenco GPL (torej mora biti odprtokodna) (Cleto, 2004). Hugo Chavez se je za prehod na OKPO (poleg varnosti in želje po neodvisnosti od ZDA in Microsofta) odločil tudi zaradi podatka, da gre 75 odstotkov cene licenčne programske opreme v druge države, 20 odstotkov za podporo tujih agencij in le pet odstotkov ostane venezuelskim programerjem (Proffitt, 2002). Podobne razloge kot Venezuela je imela za prehod še Kuba, katere lastna distribucija operacijskega sistema Nova temelji na Linuxovi distribuciji Ubuntu. Kuba se je za prehod na odprto kodo odločila predvsem zaradi varnosti in nezaupanja v Microsoftove produkte, pa tudi zaradi ameriškega embarga, ki je povzročil, da je bilo na Kubi zelo težko priti do legalnih Windowsovih operacijskih sistemov. Razlog je tudi v ideologiji. Dekan šole za prosto programje na kubanski Univerzi za informacijske znanosti Hector Rodriguez je dejal: »Gibanje prostega programja je bliže ideologiji kubanskega prebivalstva, predvsem zaradi neodvisnost in suverenosti.« (Israel, 2009) Tudi Rusija se odločila za prehod na OKPO, vendar njen prehod še poteka in se bo končal leta 2012 ali najpozneje leta 2015. Kot glavni razlog je Putin navedel željo po večji neodvisnosti od drugih držav pri uporabi lastniške programske opreme (Morozov, 2011).

Ena zanimivejših držav z vidika prehoda na OKPO je Kitajska, ki se je začela za OKPO zelo zanimati že leta 1990, leta 2005 pa je izdelala prvo različico državnega operacijskega sistema distribucije Linux, Red Flag Linux, ki se uporablja v javni upravi. Hkrati so razvili distribucijo Asianux, ki je usmerjena na azijske trge, saj podpira pismenke (Blanchard, 2007). Kitajska, katere gospodarstvo neizmerno raste, z njim pa tudi potrebe po čim bolj lokalizirani programski opremi, ki najbolj zadovolji potrebe lokalnih podjetij, z razvojem lastne programske opreme postaja konkurenčna na svetovnih trgih (Saxenian, 2003). Kitajska je imela nekdaj eno najvišjih stopenj piratstva na svetu, z uporabo OKPO pa se je to začelo manjšati. Na Kitajskem želijo s tem zagotoviti tudi večjo informacijsko varnost in neodvisnost (Lock, 2006).

Evropska unija velja za eno največjih zagovornic uporabe OKPO. Največji odprtokodni projekti in rešitve so nastali na tleh Evropske unije. Linux je naredil Finec Linus Torvalds, programski jezik Python je delo nizozemskega avtorja Guida van Rassuma, sistem upravljanja podatkovnih baz MySQL pa Šveda Michaela Wideniusa in še bi lahko naštevali (Gonzalez-Barahona, 2006). Evropska unija zelo podpira razvoj OKPO, zato so ustanovili The Open Source Observatory and Repository for European public administrations (OSOR), katerega namen je razvijati posebne aplikacije in odprtokodno programsko opremo, namenjeno uporabi v javni upravi znotraj EU. S projektom želijo zmanjšati stroške v javni upravi, standardizirati formate in postopke povsod po uniji, zmanjšati stroške e-vlade (angl. e-government) in pomagati širiti dobro prakso. OSOR financira Evropska komisija, podpirajo pa ga vlade na nacionalni, regionalni in lokalni ravni (http://www.osor.eu/about).

Na kratko še poglejmo, kje je Slovenija pri uporabi OKPO v državni javni upravi. Leta 2003 je država sprejela dokument *Politika Vlade RS pri razvijanju, uvajanju in uporabi programske opreme in rešitev, temelječih na odprti kodi*. V dokumentu lahko preberemo, da bo država podpirala uporabo odprtokodnih rešitev, jih enakopravno obravnavala skupaj z licenčnimi in podpirala izobraževanje za njihovo uporabo (mid.gov.si/mid/mid.nsf/V/.../$file/Politika_OSS_Koncna.pdf*)*. Dokument se zaenkrat še ni uveljavil v praksi. Do letos je država na podlagi raziskave *Ocena ekonomske upravičenosti MS EA za obdobje 2003–2005* (e-uprava.gov.si/eud/e.../Studija%20upravicenosti%20MS%20EA.pdf*)*, ki je ugotavljala, da je licenčna programska oprema finančno bolj smotrna od OKPO, za javno upravo prek javnih naročil kupovala licenčno programsko opremo MS Office. So pa v javni upravi tudi svetle izjeme, kot je na primer Vrhovno sodišče RS, na katerem so v letih 2006 in 2007 opravili prehod in zamenjali pisarniški paket MS Office z Open Office, Microsoftov spletni brskalnik Internet Explorer z Mozilla Firefox in na 4600 delovnih postaj namestili odprtokodno aplikacijo za spletno pošto Thunderbird. Vrhovno sodišče ugotavlja, da na leto tako prihrani približno 400.000 evrov (http://www.finance.si/305469/Sodi%B9%E8a-z-odprto-kodo-prihranijo-400-tiso%E8-evrov-letno/rss1).

Leto 2011 je na tem področju v Sloveniji prelomno, saj je na začetku leta država objavila študijo, s katero izraža namero, da bi do leta 2015 postopoma prešla na

uporabo OKPO; sprva zgolj z zamenjavo MS Office z Open Office, sčasoma pa bi morda zamenjali vse operacijske sisteme z odprtokodnimi, kot so Linuxove distribucije (mju.gov.si/.../Studija_uvajanja_OKPO_na_DP_v_JU_koncna_razlicica_17.2.2011.pdf). Študija je sprožila velik plaz kritik, predvsem ponudnikov licenčnih programskih rešitev, v Microsoftu pa so izjavili, da bi jim takšna odločitev vlade prinesla vsaj 2,5 milijona evrov izgube na leto (Mihajlovič, 2011).

Slovenija je pri uveljavljanju in uporabi OKPO v primerjavi z drugimi državami EU precej zaostala. Vendar je treba tu izpostaviti tudi morebitno problematiko, če bi prišlo do prehoda slovenske državne javne uprave na OKPO. Problematične so aplikacije, narejene posebej za uporabo v javni upravi – narejene so namreč le za Microsoftovo okolje. Do podobnih težav so prišli tudi v drugih državah, saj so morali aplikacije, ki so bile posebej narejene za Microsoftovo okolje, in programe ponovno narediti ali pa jih spremeniti ter omogočiti podporo tudi na drugih operacijskih sistemih in združljivost z drugačnimi formati, kar je povečalo stroške (Souza, 2006).

Znani so primeri prehodov z OKPO nazaj na zaprtokodno programsko opremo. Zelo znan prehod nazaj na Windows Vista je z Dunaja, kjer so se leta 2005 odločili razviti svojo distribucijo, temelječo na Debian Linux, imenovano Wienux. Med glavnimi težavami je bil program Schlaumäuse, ki je bil narejen leta 2003 in namenjen računalniškemu izobraževanju otrok. Program je bil narejen zgolj za okolje Internet Explorer in ni podpiral odprtokodnega programa Firefox. Podjetje, ki je razvilo program, je predvidelo podporo za Firefox šele leta 2009. Dunaj se je zato leta 2008 odločil preiti nazaj na Windows (Mobility, 2008).

Zadnji tak prehod je naredilo nemško zunanje ministrstvo, ki je leta 2005 prešlo na OKPO. Na namizne računalnike so namestili distribucijo Debian Linux. S prehodom so želeli prihraniti denar, ki bi sicer šel za licenčnine. Leta 2007 so v poročilu zapisali, da so s prehodom resnično znižali stroške. Leta 2011 pa so javno najavili, da prehajajo nazaj na MS Windows in MS Office. Kot razlog so navedli pomanjkljivo podporo strojni opremi, kot so tiskalniki in podobno. Stroški se po njihovem mnenju niso zmanjšali, saj so morali veliko denarja vložiti v razvoj lastnih gonilnikov za tiskalnike. Prav tako so se uporabniki pritoževali nad pomanjkanjem funkcij in slabo interoperabilnostjo. Prehod nazaj na MS Windows jih bo po njihovem mnenju stal manj, ker jim ne bo treba plačevati programerjev za razvoj gonilnikov (http://www.h-online.com/open/news/item/No-more-desktop-Linux-systems-in-the-German-Foreign-Office-1191122.html).

4 INFORMACIJSKA VARNOST IN VLOGA OKPO

Vedno pogosteje dobivamo novice o novih kibernetičnih napadih po svetu. Največ pozornosti so deležni napadi, ki potekajo med ZDA in Kitajsko. Vendar kibernetični boji potekajo tudi med mnogimi drugimi državami, saj jim ta asimetrični način bojevanja omogoča dosegati cilje z malo napora in predvsem brez uporabe sile,

čeprav so posledice takšnih napadov lahko tudi hujše (primer Stuxnet). Po podatkih poročila McAfee danes več kot 120 držav razvija ali ima kibernetična orožja za napade na finančne trge, državne računalnike, vojaške baze ... Tipi napadov so različnih vrst, od DDOS in vdorov v sisteme do kraje podatkov. Zaradi povečanega števila napadov je vedno več držav uvedlo posebne centre (poleg CERT), da bi se ob napadih komunikacija med prizadetimi udeleženci izboljšala oziroma bi se na napade hitreje odzvali. Za reševanje te problematike ni enotnega pristopa – vsaka država ima svojega. Deljena so tudi mnenja o tem, kdo naj ima ob napadu na voljo informacije o njem in koliko naj jih bo. Nekateri menijo, da je boljša izključitev javnosti, medtem ko drugi priporočajo čim večjo preglednost (Baker, 2009).

OKPO ima lahko ob napadu veliko moč na defenzivni ravni. Splet zaradi njegove anarhične narave velikokrat poimenujemo »divji zahod« (Baker, 2009). A podobno kot na divjem zahodu se tudi tu vsak posameznik zavaruje s svojim orožjem. Varnost se ob kibernetičnih napadih ne začne na ravni države, temveč na ravni njenih prebivalcev.

Na področju informacijske varnosti prevladujeta dva pristopa, tako imenovana *top-down* in *bottom-up*. Pristop *top-down* izvira iz koncepta nacionalne varnosti in temelji na stvarnosti, v ospredje postavlja državo in njeno vlogo pri pisanju ter sprejemanju zakonodaje, smernic in strategij na področju informacijske varnosti. Za varnost posameznika na področju informacijsko-komunikacijske tehnologije (IKT) mora poskrbeti država, vendar pa lahko državo posredno ali neposredno ogrožajo tudi posamezniki (Svete, 2005). Slabost takšnega sistema je, da zakonodaja zaostaja za prakso in da države v praksi težko ščitijo posameznike na področju varnosti IKT.

Pristop *bottom-up* izvira iz koncepta človekove varnosti, iz liberalistične in konstruktivistične teorije. V ospredje postavlja posameznika z njegovimi vrednotami in interesi. Posameznik na tem področju ni zgolj žrtev, ki jo mora država ščititi, temveč izjemno pomemben dejavnik znotraj informacijske varnosti, ki lahko s svojim delovanjem nanjo močno vpliva. Nevešč posameznik lahko na področju IKT zelo ogrozi varnost, po drugi strani pa lahko zelo vešč k njej veliko prispeva (Svete, 2005).

OKPO na področju informacijske varnosti predstavlja pristop *bottom-up*, saj vsakemu posamezniku daje možnost nadzora nad lastnim sistemom. Za njegovo varnost je odgovoren posameznik, pomembna pa je tudi vloga odprtokodne skupnosti, ki javno opozarja na nevarnosti.

Diver (2007) vidi idealen sistem v kombinaciji obeh pristopov. Države potrebujejo strateške usmeritve in zakonodajo na področju informacijske varnosti, vendar je dobro tudi, da imajo informacijsko bolj vešče posameznike, ki dobro skrbijo za varnost sistema in s tem preprečujejo morebitno širjenje zlonamerne programske opreme.

Sklep OKPO je z leti postala resna konkurenca zaprtokodnim sistemom in prevladuje tako na področjih superračunalnikov kot strežnikov. Rast so opazile tudi države, ki so se med gospodarsko krizo za prehod na OKPO odločile zaradi zmanjšanja stroškov, medtem ko so se nekatere za prehod odločile predvsem zaradi varnosti, nezaupanja v Microsoftove izdelke in v želji po večji neodvisnosti.

Varnost je relativna. V vsak sistem je mogoče vdreti, zato ne moremo trditi, da je nek sistem boljši, drugi pa slabši. Moja hipoteza je bila, da je odprtokodna oprema varnejša od zaprtokodne. Hipotezo delno potrjujem. OKPO ima dobre varnostne mehanizme, vendar je njihova varnost v praksi odvisna predvsem od njenih uporabnikov. OKPO omogoča večjo preglednost in možnost vpogleda v izvorno kodo, vendar to zanima malo ljudi. Večina ljudi uporablja računalnik za preproste zadeve, kot je pisanje dokumentov. Varnost zaupajo razvijalcem OKPO in sistemu *veliko oči*, oba sistema pa v praksi kažeta, da preveč temeljita na zaupanju. Znanih je veliko primerov, ko ranljivosti v sistemu niso bile odkrite več let. Na drugi strani imamo zaprtokodne sisteme, ki običajnemu uporabniku ne omogočajo vpogleda v izvorno kodo in nimajo sistema *veliko oči*. Podobno kot pri OKPO tu varnost temelji na zaupanju do razvijalcev. Razlika med OKPO in zaprtokodnimi sistemi je zgolj v preglednosti, vendar žal oba temeljita na zaupanju ljudi v njuno varnost. Številne države so se zato odločile za OKPO, ker jim omogoča, da izvorno kodo pregledujejo same, poleg tega pa razvijajo opremo, ki je narejena posebej zanje.

Prednost OKPO pred zaprtokodnimi sistemi vidim predvsem na področju javnega objavljanja ranljivosti in hitrega popravljanja pomanjkljivosti.

OKPO ima dobre varnostne mehanizme in omogoča večjo preglednost, za ogroženost sistema pa je še vedno najbolj odgovoren človek. Večina uporabnikov ni vešča uporabe računalnikov. Takšni uporabniki ogrožajo varnost svojih in tujih sistemov, ker ne uporabljajo antivirusnih programov in svoje računalnike neredno posodabljajo.

Hipotetično bi k večji informacijski varnosti OKPO lahko pripomogel pristop *bottom-up*, vendar le, če bi bili vsi uporabniki vešči uporabe računalnikov, če bi znali brati izvorno kodo in iskati ranljivosti, ki bi jih javno objavljali. Takšna pričakovanja so utopična, zato težko trdimo, da je OKPO z varnostnega vidika boljša – ne glede na varnost sistem še vedno ogroža človek.

Trenutno se zaradi svetovne gospodarske krize mnoge države odločajo za prehod na OKPO, predvsem zaradi zmanjšanja stroškov. Tudi Slovenija je med njimi. Na tej točki je nujno izpostaviti morebitne izzive, ki bi se lahko pojavili ob prenagljenem in premalo premišljenem prehodu. Veliko se lahko naučimo iz primerov Nemčije in Dunaja (prehod nazaj na zaprtokodne sisteme zaradi strojne opreme, ki OKPO ne podpira). Zagotoviti bi bilo treba združljivost OKPO in sedanje (ali v prihodnosti načrtovane) strojne opreme – ena izmed možnosti je na primer popis sedanje strojne opreme in preverjanje, kako jo podpira OKPO. Ob morebitni ugotovitvi, da ni podprta, bi bilo treba proučiti stroške razvoja ustreznih gonilnikov. Morda je

največji izziv v programski opremi, ki je pisana zgolj za okolje Windows. Treba bi bilo proučiti stroške razvoja popravkov, ki bi omogočali podporo OKPO, in tudi čas za njihovo izdelavo. Smiselno bi bilo tudi pregledati sedanje distribucije in najti slovenskemu prostoru najustreznejšo (mogoč pa je tudi razvoj domače).

Če Slovenija morebitnega prehoda na OKPO ne bo zastavila premišljeno, se nam lahko zgodi, da se prehod tudi ne bo obrestoval. V Sloveniji je izjemno malo literature na to temo, prav tako znanstvenih člankov in študij. V prihodnje bi bilo koristno opraviti več neodvisnih analiz stroškov in koristi, ki bi ugotavljale smotrnost prehoda Slovenije na OKPO.

Literatura

1. *Baker, S., 2009. In the Crossfire: Critical Infrastructure in the Age of Cyber War. Santa Clara: McAfee, Inc. http://tinyurl.com/3l6k4bm (3 August 2011).*
2. *Blanchard, J. F., 2007. China, multinational corporations, and globalization: Beijing and Microsoft battle over the opening of China's gates. Seoul: Asian perspective. Institute for Far Eastern Studies. http://tinyurl.com/3vb97m4 (2 April 2011).*
3. *Campbell, D., 1999. NSA Backdoor Into Windows. http://tinyurl.com/3k3e4d (12 April 2011).*
4. *Chuvakin, A., 2003. An Overview of Unix Rootkit. Chantilly: iDEFENSE Inc. http://tinyurl.com/42gbmjd (10 September 2011).*
5. *Cleto, S., 2004. Venezuela Embraces Linux and Open Source Software, but Faces Challenges. http://tinyurl.com/3dqh9ns (3 May 2011).*
6. *Diver, S., 2006. Information Security Policy - A Development Guide for Large and Small Companies. Washington: SANS Institute. http://tinyurl.com/3suc5tc (17 September 2011).*
7. *Espiner, T., 2006. Trend Micro: Open source is more secure. http://tinyurl.com/3c6u6cz (20 May 2011).*
8. *Espiner, T., 2010. Microsoft opens source code to Russian secret service. http://tinyurl.com/2w8moaq (3 August 2011).*
9. *Geer, D., in drugi, 2003. CyberInsecurity: The Cost of Monopoly How the Dominance of Microsoft's Products Poses a Risk to Security. http://tinyurl.com/63bhse8 (18 September 2011).*
10. *Germain, J. M., 2008. Linux: A Tempting Target for Malware?. http://tinyurl.com/65jn5vu (1 May 2011).*
11. *Gonzalez-Barahona, J., Robles, G., 2006. Libre Software in Europe. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 161–188.*
12. *Humbery, B., 2011. The Evolution of the Personal Package Archive system. http://tinyurl.com/3tqw8rq (20 May 2011).*
13. *Jose, M., 2011. The Goal is 200 Million Ubuntu Users in 4 Years - Mark Shuttleworth at UDS. http://tinyurl.com/3cd4p67 (23 May 2011).*
14. *Kalkuhl, M., 2009. Malware beyond Vista and XP. http://tinyurl.com/3qemfbs (20 May 2011).*
15. *Kimberly, S., 2005. The value of open standards and open-source software in government environments. Austin: IBM SYSTEMS JOURNAL. Volume 44 Issue 2, January 2005. http://tinyurl.com/3qsatqt (12 May 2011).*
16. *Koetzle, L., 2004. Is Linux More Secure Than Windows? http://tinyurl.com/3p9uue8 (20 May 2011).*
17. *Kovačič, M., 2006. Kriptografija, anonimizacija in odprta koda kot boji za svobodo na internetu. Javnost- the public. Vol. 13. (2006). Fakulteta za družbene vede, Univerza v Ljubljani, p. 93–110.*

18. *Laurie, B., 2006. Open Sources and Security. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 57–71.*
19. *Lewis, J., 2006. Government Open Source Policies – August 2007. Washington: Center for Strategic and International Studies. http://tinyurl.com/3mhva3y (12 May 2011).*
20. *Lock, B. Y., Liu L., Saxena S., 2006. When China Dances with OSS. V C. DiBona, ed. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 197–210.*
21. *Meintjes, T., 2011. Is a virus or malware infection the cause of your slow computer? http://tinyurl.com/442u5se (26 May 2011).*
22. *Mihajlovič, N., 2011. Microsoft gre nad Pahorja, zdaj hoče pošteno konkurenco. http://tinyurl.com/3lxz4va (24 May 2011).*
23. *Mobility, T., 2008. Vienna failed to migrate to GNU/Linux: why?. http://tinyurl.com/6mktzl (9 September 2011).*
24. *Morozov, E., 2011. A Walled Wide Web for Nervous Autocrats. http://tinyurl.com/2vflb3c (29 May 2011).*
25. *O'Dowd, D., 2004. Linux Security Controversy. http://www.ghs.com/linux/security.html (18 September 2011).*
26. *Peeling, N., Satchell, J., 2001. Analysis of the Impact of Open Source Software. http://tinyurl.com/6lyeod8 (19 May 2011).*
27. *Poulsen, K., 2001. Borland Interbase backdoor exposed. Open source reveals foolishly hardcoded password. (12 May 2011).*
28. *Proffitt, B., 2002. Venezuela's Government Shifts to Open Source Software. http://tinyurl.com/3j9kqzo (15 May 2011).*
29. *Sapronov, K., 2007. Kaspersky Security Bulletin 2006: Malware for Unix-type systems. http://tinyurl.com/3vuu2k3 (23 May 2011).*
30. *Saxenian, A., 2003. Government and Guanxi: The Chinese Software Industry in Transiton. Berkeley: University of California at Berkeley. http://tinyurl.com/3u37nwl (12 May 2011).*
31. *Schneier, B., 2002. Secrecy, Security, and Obscurity. Crypto-Gram. http://tinyurl.com/5rk6jaw (17 May 2011).*
32. *Schneier, B., 2006. Microsoft Vista's Endless Security Warnings. http://tinyurl.com/ges4k (23 May 2011).*
33. *Souza, B., 2006. How Much Freedom Do You Want. V C. DiBona, ur. Open Sources 2.0: The Continuing Evolution. O Reilly Media, p. 211–229.*
34. *Svete, U. 2005. Varnost v informacijski družbi. Ljubljana: Fakulteta za družbene vede.*
35. *Weber, S., 2004. The success of open source. Cambridge: Harward University Press.*
36. *Wynants, M., 2005. Free as in Freedom, not Gratis!. V Wynants, M., Cornelis J., ed. How Open is the Future? Economic, Social & Cultural Scenarios inspired by Free & Open-Source Software. Brussels: Brussels University Press, p. 69–85.*

Viri:

1. *http://distrowatch.com/ (26 May 2011).*
2. *http://librenix.com/?inode=21 (23 April 2011).*
3. *http://support.apple.com/kb/ht1528 (26 May 2011).*
4. *http://tinyurl.com/27l5wvh (26 May 2011).*
5. *http://tinyurl.com/28lpgq (28 May 2011).*
6. *http://tinyurl.com/3f69g8u (19 May 2011).*
7. *http://tinyurl.com/3fldnhr (26 May 2011)*
8. *http://tinyurl.com/3hdqvgd (20 May 2011).*
9. *http://tinyurl.com/3pdksvv (20 May 2011).*
10. *http://tinyurl.com/44x9pxd (26 May 2011).*
11. *http://tinyurl.com/5s4k3ry (10 September 2011).*

12. *http://tinyurl.com/68u2cm7 (12 April 2011).*
13. *http://tinyurl.com/6gyjnou (20 May 2011).*
14. *http://tinyurl.com/6hszcy5 (20 May 2011).*
15. *http://tinyurl.com/6jgg3ut (20 April 2011).*
16. *http://tinyurl.com/hdpo9 (18 September 2011).*
17. *http://tinyurl.com/o4foa (3 May 2011).*
18. *http://www.Linuxfordevices.com/ (20 April 2011).*
19. *http://www.osor.eu/about (20 May 2011).*
20. *https://bugs.launchpad.net/ubuntu/ (18 September 2011).*

Anže Rode,
Kristian Bernšak,
Bojan Langerholc

DOI:10.33179/BSV.99.SVI.11.CMC.13.3.5.PREV

Strokovni članek

ENOTA ZA SPECIALNO DELOVANJE SLOVENSKE VOJSKE – ODGOVOR NA SODOBNE IZZIVE

THE SAF SPECIAL OPERATIONS UNIT RESPONSE TO MODERN CHALLENGES

Professional article

Povzetek Enota za specialno delovanje (ESD) zagotavlja zmogljivosti specialnega delovanja Slovenske vojske in uresničevanje posebnih nacionalnovarnostnih ciljev Republike Slovenije.
Visoka usposobljenost, sposobnost prikritega delovanja, zmožnost velike natančnosti zaradi zmanjševanja stranskih učinkov in visoka prilagodljivost glede na različne vire ogrožanja so samo nekatere značilnosti, ki poudarjajo vlogo in pomen ESD znotraj oboroženih sil. Te značilnosti omogočajo njeno uporabo za izpolnjevanje obveznosti Republike Slovenije do sistema kolektivne obrambe zveze Nato ter zagotavljanje mednarodne varnosti znotraj OZN v mednarodnih operacijah in na misijah, ko drugih enot ter virov Slovenske vojske ni mogoče uporabiti. Hkrati je ESD potencialna zmogljivost za obrambo države in delovanje v posebnih kriznih razmerah protiterorističnega delovanja v Republiki Sloveniji.
ESD je s potrditvijo svojih zmogljivosti v praksi pokazala, da so predlagani teoretični koncepti in rešitve, na katerih temelji, pravilni in uresničljivi, ESD pa vrhunsko usposobljena enota, ki predstavlja ost enot za bojno delovanje Slovenske vojske.

Ključne besede ***Specialno delovanje, protiterorizem, protiuporništvo, Nato, Enota za specialno delovanje, na učinkih temelječe operacije.***

Abstract The Special Operations Unit (SOU) provides special operations capabilities for the Slovenian Armed Forces (SAF) and the implementation of special national security objectives for the Republic of Slovenia.
Specialized training, the ability to perform covert operations, high accuracy to achieve collateral damage reduction, and great flexibility in facing different sources of threat are but a few of the features that highlight the role and importance of the Special Forces units of the armed forces. Having such characteristics, the unit can be used to fulfil the obligations of the Republic of Slovenia to NATO's collective defence system and ensure the international security of UN missions when no other

SAF units and capabilities can be employed. At the same time, the SOU provides potential capabilities for national defence and specific crisis situations for counter-terrorism activities in the Republic of Slovenia.

By validating its capabilities in practice, the SOU has shown that the theoretical concepts on which it is based are both good and feasible. It has proved itself to be a highly qualified unit – the elite of the SAF's combat operations units.

Key words ***Special Forces, special operations, counter-terrorism, counter-insurgency, NATO, Special Operations Unit, effects-based operations.***

Uvod

Spremenjene grožnje in narava konfliktov v obdobju po hladni vojni ter projekcija prihodnjega varnostnega okolja zahtevajo od držav in organizacij (npr. OZN, EU, Nata in drugih) drugačen in predvsem učinkovitejši način soočanja s temi izzivi[1]. Grožnje in izzivi imajo seveda pomembne implikacije ter zahtevajo tudi pomembne spremembe v varnostnih sistemih in oboroženih silah – vključno s specialnimi silami.

Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2025 – ReSDPRO SV 2025 (2010, str. 7) navaja, /…/ *da se je v evro-atlantskem prostoru močno zmanjšala verjetnost izbruha oboroženih meddržavnih spopadov. Vojaške grožnje se bodo pojavljale predvsem v obliki lokalnih in regionalnih nestabilnosti, ki lahko hitro prerastejo svoj okvir. Sodobne grožnje prevzemajo vse bolj hibridno obliko, njihov značaj pa zaradi močnih globalizacijskih vplivov postaja večplasten in mednaroden, takšni pa so tudi njihovi učinki. Bojišče prihodnosti bo poleg kopnega, morja in zraka obsegalo tudi kibernetski prostor in vesolje*.

Avtorji tako menimo, da bo varnostno okolje prihodnosti postalo še bolj zapleteno zaradi kombinacije različnih elementov: večjih ubojnih zmožnosti sodobnega orožja, razvoja sredstev za hitro premikanje vojaških sil, mednarodnega terorizma[2], širjenja orožja za množično uničevanje, lažjega dostopa do informacij, prisotnosti medijev ipd. Z vojaškimi strukturami in metodami[3], ki so ustrezale reševanju meddržavnih konfliktov, ne bo mogoče obvladovati zahtevnih varnostnih razmer 21. stoletja.

---

[1] *Prevladujoče stališče med različnimi obrambnimi in varnostnimi subjekti v svetu je, da sedanje in prihodnje varnostno okolje pred nas postavljata zapletene izzive, ki jih je težko predvideti. Zelo raznolike in nekonvencionalne grožnje lahko ogrozijo širšo mednarodno stabilnost in povzročijo trajno konfliktno stanje. Specialne sile so dejaven instrument, ki je idealno prilagojen nejasnemu in dinamičnemu okolju, po drugi strani pa ohranja svobodo delovanja z uporabo načela varčnosti sil. Dodatno imajo specialne sile posebno zmožnost za izvedbo nalog v okoljih, v katerih so konvencionalne sile v primerjavi s specialnimi v strateško ali operativno slabšem položaju (NATO Special Operations Study, 2008).*

[2] *Terorizem je tipičen primer sodobne asimetrične grožnje, pri čemer Prezelj (2007, str. 67) ugotavlja, »/.../ da se asimetrija nanaša na neproporcionalnost subjekta, ki ogroža (nedržavni akterji proti državi), sredstev, ki jih uporablja, in posledic (minimalni vložek – maksimalni rezultati, ki na primer presegajo neposredne posledice bombne eksplozije).«*

[3] *Seveda je lahko ESD le segment v celovitem odzivu sodobne države na terorizem (Prezelj, 2007, str. 68) in dopolnjuje skupno dejavnost in odziv države (skupna slika).*

Tako Srednjeročni obrambni program 2007–2012 (SOPR) iz leta 2006 nakazuje, da bodo na prihodnje strateško varnostno okolje bistveno vplivali: globalizacija, sofisticirana ubojna sredstva in različne oblike asimetričnega vojskovanja, hitro se spreminjajoče varnostne razmere, demografski in politični dejavniki ter pomanjkanje virov, ki povzročajo množične migracije prebivalstva, razmah radikalnih ideologij, nerešene meddržavne in notranje konflikte ter naravne nesreče večjih razsežnosti. SOPR predvideva tudi, da bodo zaradi globalizacije zahodne demokracije, še posebej njihove ekonomije, vse bolj občutljive na stabilnost v različnih delih sveta, ki bo posredno ali neposredno vplivala na njihov ekonomski interes in delovanje prostega trga.

Informacijska omrežja že danes omogočajo pregled nad dogajanji kjer koli na svetu in v realnem času. To dejstvo bodo v prihodnje z informacijskimi strategijami izkoriščali različni akterji, tudi taki, katerih glavni namen je uničevalno delovanje. Zaradi vse bolj preprostega in razširjenega dostopa do sodobnih in naprednih tehnologij bodo teroristični in drugi napadi vse bolj učinkoviti. Vse bolj izrazita bo grožnja možnosti dostopa do tehnologij in sredstev za množično uničevanje, ki jih bodo sponzorirale tudi države (SOPR 2007–2012).

Razkorak med razvitimi in nerazvitimi državami bo še naprej povzročal etnične konflikte ter množične migracije. Gospodarske in finančne krize bodo povzročale pritisk in razkrajale socialne sisteme (SOPR 2007–2012).

Zahteve po energetskih virih, vodi in hrani bodo naraščale, podnebne spremembe pa bodo negativno vplivale na možnosti za zagotavljanje vode in hrane. Zaradi degradacije okolja se bo verjetno povečalo število naravnih nesreč, ki bodo dolgoročno vplivale na socialne in ekonomske razmere v nekaterih delih sveta. Naraščala bosta organizirani kriminal in siromaštvo, pojavljale se bodo nove bolezni in lakota (SOPR 2007–2012).

Izvor ogrožanja bodo nestabilne države, slabo upravljanje virov in nenehno tekmovanje zanje. Nerešeni konflikti ter skupine in države, ki podpirajo radikalne ideologije, bodo predstavljali grožnje, ki lahko dosežejo globalne razsežnosti. Tako lahko nekatere hujše oblike navedenih groženj v temeljih zamajejo globalno stabilnost (Rode, 2007, str. 5).

Strateško presenečenje je mogoče in zanj bo malo ali nič predhodnih opozoril. Zato bo sodelovanje v Natu pomembno, hkrati pa realna možnost, da se sproži institut kolektivne obrambe.

Razmere na Balkanu bodo tudi v prihodnje nestabilne. Problematično ostaja predvsem Kosovo. Kljub temu se bodo mednarodne sile, ki zagotavljajo stabilnost na Kosovu in v BiH, prestrukturirale in zmanjšale. Proces širitve Nata in EU na južne balkanske države pa se bo nadaljeval.

Varnostne razmere v Afriki bodo tudi v prihodnje kritične, nanje pa bodo vplivali različni dejavniki, kot so hitra demografska rast prebivalstva, epidemije, revščina, lakota, pomanjkanje vode, nestabilni režimi, propadle države, medverska in medetnična trenja itn. Ti dejavniki in razmere, ki jih bodo ustvarjali, bodo povzročali ilegalne migracije v Evropo ter razraščanje terorističnih skupin, ki bodo svoje delovanje usmerjale tudi v Evropo (SOPR 2007–2012). Zaenkrat pa tako imenovana arabska pomlad v Tuniziji, Egiptu, Libiji in drugje še ni potrdila črnogledih napovedi.

Bližnji vzhod bo ostal krizno žarišče, na katerem se bodo nadaljevali medetnični in medverski spopadi, širjenje različnih oblik fanatizma ter posledično terorističnih delovanj, ki se lahko usmerijo tudi v evropske države (SOPR 2007–2012).

Spekter vojskovanja bo v prihodnosti usmerjen v krize, v katerih je lahko uporabljeno jedrsko in drugo orožje za množično uničevanje, v klasične meddržavne spopade, notranje konflikte, ki povzročajo propad držav, v terorizem in druge krizne razmere. Poseben izziv bo dejstvo, da se v različne dimenzije vojskovanja ne vključujejo zgolj oborožene sile, pač pa različni akterji: državni, mednarodni, nevladni in lokalni ter vsi elementi različnih instrumentov moči, kot so politični, vojaški, informacijski, ekonomski in drugi.

Na vojaške grožnje država običajno odgovori z oboroženimi silami. Tako bodo v prihodnje tudi enote SV z nadaljevanjem procesa integracije v zavezništvo prevzemale vse večje obveznosti, ne le v smislu velikosti in številčnosti sodelujočih enot, temveč tudi v smislu kompleksnosti in težavnosti dodeljenih nalog.

1 NATO, SLOVENSKA VOJSKA IN SPECIALNE SILE (SPECIAL OPERATIONS FORCES – SOF)

Na podlagi spoznanj in izkušenj, predvsem iz operacij specialnih sil v Afganistanu, je bila leta 2006 na vrhunskem zasedanju Nata v Rigi sprejeta odločitev o preoblikovanju specialnih sil zveze (NATO SOF Transformation Initiative) za doseganje večje medsebojne primerljivosti in zmožnosti skupnega delovanja. Ta cilj naj bi bil dosežen predvsem s skupnim usposabljanjem, opremljanjem ter z uvedbo in doseganjem skupnih standardov. S tem namenom je bil leta 2007 ustanovljen tudi Koordinacijski center za specialne operacije zveze Nato (NATO SOF Coordination Centre – NSCC), ki se je na začetku leta 2010 preoblikoval v Poveljstvo za specialno delovanje zveze Nato (NATO Special Operations Headquarters – NSHQ). Pozneje je postal tudi edino telo za vodenje in usklajevanje specialnih operacij Nata, namenjeno optimizaciji uporabe specialnih sil zavezništva in zagotavljanju zmogljivosti operativnega poveljevanja skladno z usmeritvami SACEUR (glej Beršnak, 2010, str. 27–28).

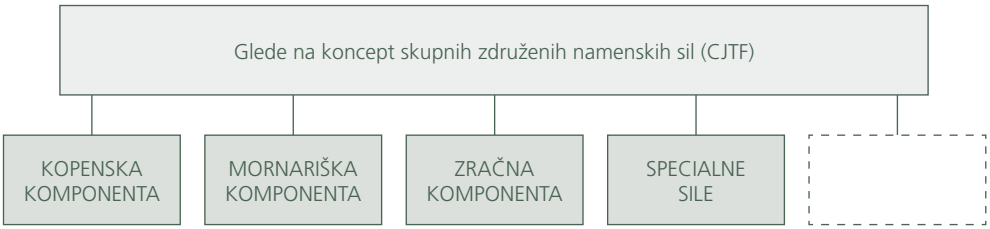
Kot navaja Paternus (2010, str. 70) je Severnoatlantski svet leta 2006 kot izhodišče za uvedbo skupnih standardov sprejel dokument MC 437/1 Special Operations Policy, ki predstavlja temelj za oblikovanje skupne Natove doktrine za specialne operacije. Leta 2008 je bil začet proces ratifikacije AJP 3.5, Allied Joint Doctrine for Special

Operations, ki je bil končan leta 2009, ko je bil dokument tudi ratificiran kot SVS STANAG 2523(1).

Dva najpomembnejša dokumenta o področju specialnih sil sta prav MC 437/1 Special Operations Policy in AJP 3.5, ki opredeljujeta pomen in namen specialnih sil v nacionalni in kolektivni obrambi, organizacijske modele, finančni vidik, minimalne zahtevane zmogljivosti itn.

Vojaška doktrina Slovenske vojske definira specialne sile kot eno izmed komponent skupnih združenih namenskih sil (Combined Joint Task Force – CJTF) (slika 1), ki se organizirajo glede na svoje poslanstvo, združeno območje delovanja ter prevladujoči način delovanja. Skupne združene namenske sile poleg specialnih sil vključujejo še zračno, mornariško in kopensko komponento (glej Furlan idr., 2006, str. 29).

Slika 1: Skupne združene namenske sile (Furlan idr., 2006, 29)



Specialne sile SV so nosilec specialnega delovanja, ki /…/ *je način bojnega delovanja posebej izbranih, opremljenih, organiziranih in usposobljenih enot Slovenske vojske. Te ga izvajajo z namenom podpore doseganju vojaških, političnih ali psiholoških ciljev, ki imajo operativni ali strateški pomen. Specialno delovanje obsega nekonvencionalne vrste bojnega delovanja, direktne akcije, specialno izvidovanje, obveščevalno dejavnost, protiteroristično delovanje, psihološko delovanje ter bojno iskanje in reševanje. Vse aktivnosti specialnih sil so usmerjene v vojaške cilje*. (Furlan idr., 2006, str. 50)

Furlan (idr. 2006, str. 50) je opredelil, da so značilnosti uporabe specialnih enot Slovenske vojske /…/ *delovanje v manjših skupinah, samostojno, na večjih globinah in v daljšem časovnem obdobju ter prikritost delovanja. Svoje naloge izvajajo pri ofenzivnem, defenzivnem, informacijskem in stabilizacijskem delovanju Slovenske vojske. V okoliščinah, ko sovražnik zasede in nadzira del ozemlja Republike Slovenije, specialne in druge enote Slovenske vojske izvajajo nekonvencionalne vrste bojnega delovanja s poudarkom na gverilski taktiki. Enote se preoblikujejo v manjše skupine, katerih cilj je nenehno motenje, uničevanje, nevtraliziranje in zmanjšanje morale sovražnika. Bojno delovanje je samostojno, agresivno, prikrito, inovativno, neprekinjeno in sili sovražnika v vzdrževanje statične razporeditve, pri čemer se povečuje manevrski prostor Slovenske vojske. Enote se izogibajo frontalnemu bojevanju. Napadalnost in presenečenje sta temeljni načeli, po katerih enote izvajajo bojna delovanja na zasedenem ozemlju*. (Furlan idr., 2006, str. 51–52)

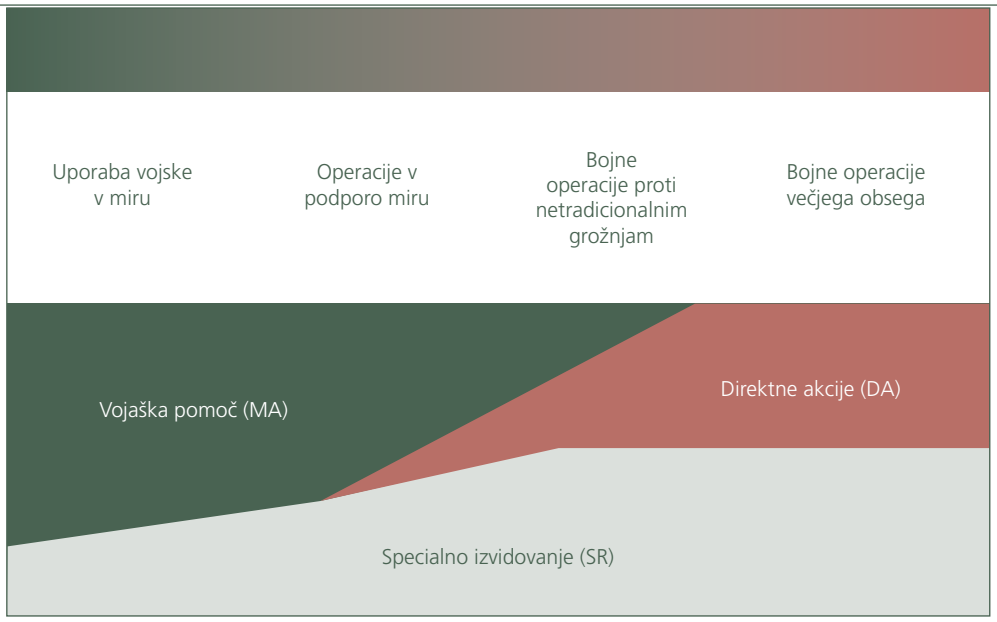
2 NALOGE NATOVIH SPECIALNIH SIL

2.1 Osnovne naloge Natovih specialnih sil

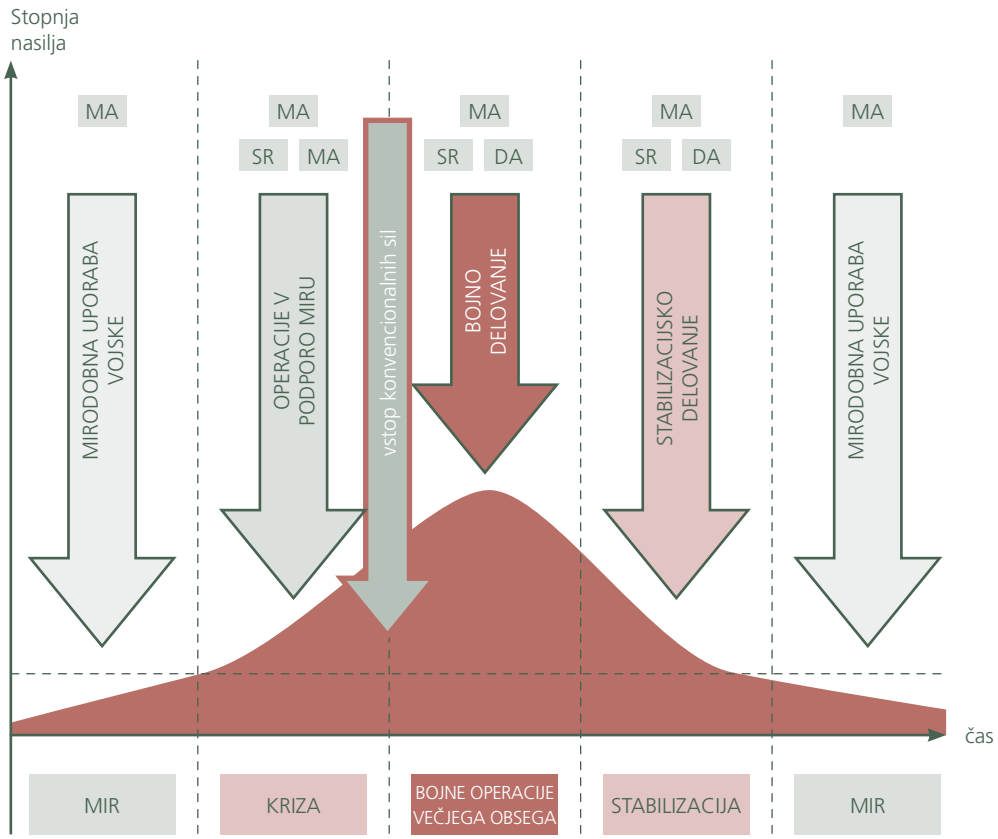
SVS STANAG 2523(1), Združena zavezniška doktrina specialnih operacij, opredeljuje osnovne naloge Natovih specialnih sil (v nadaljevanju naloge), in sicer:

- **specialno izvidovanje** (Special Reconnaissance – SR), to so aktivnosti zbiranja obveščevalnih podatkov, ki dopolnjujejo nacionalne ter zavezniške obveščevalne vire in sisteme s pridobivanjem posebnih, natančno določenih in časovno pomembnih informacij na operativni in strateški ravni. Ko v oteženih okoliščinah (velika aktivnost sovražnika, zahteven teren ipd.) izvidniško-obveščevalni organi v konvencionalnih silah ne morejo pravočasno zagotoviti natančnih in časovno pomembnih podatkov, se uporabijo specialne sile;
- **neposredne akcije** (Direct Action – DA) dopolnjujejo Natove zmožnosti z napadi na posebne, točno določene cilje strateškega ali operativnega pomena, po svojem obsegu in času delovanja so omejene. Glavni načini izvajanja teh akcij so: diverzije, naskoki, zasede, usmerjanje delovanja ognjene podpore z zemlje, iz zraka in z morja ter usmerjanje »pametnega orožja« (npr. lasersko vodenih bomb);
- **vojaška pomoč** (Military Assistance – MA) obsega zelo različne ukrepe podpore prijateljskim ali zavezniškim silam. Specialne sile lahko v okviru vojaške pomoči sodelujejo pri usposabljanju, opremljanju, podpori in uporabi (delovanju) drugih sil.

Koncept razporeditve osnovnih nalog specialnih sil oziroma načelna razmerja med izvajanjem teh nalog med konfliktom so razvidna s slike 2, medtem ko slika 3 prikazuje načelni spekter izvajanja nalog v sklopu Natovega sistema kriznega upravljanja.



Slika 2: NATO SOF in spekter konflikta (Newton, 2010)



Slika 3: Natov sistem kriznega upravljanja in naloge SOF

2.2 Druge naloge Natovih specialnih sil

Poleg osnovnih opredeljuje SVS STANAG 2523(1) še druge naloge, v katerih sodelujejo specialne sile zavezništva (niso pa izključni akter), in sicer:

– podpora v boju proti neregularnim aktivnostim sovražnika – vključuje protiteroristično[4] in protiuporniško delovanje[5] v operacijah zavezništva;
– reševanje talcev – specialne sile lahko sodelujejo v teh delovanjih pod posebnimi pogoji.

Pomembno je poudariti, da ESD kljub svojim zmogljivostim nima zakonskih pooblastil za take aktivnosti na območju Republike Slovenije, zanje imata zakonska pooblastila Policija s Specialno enoto in Vojaška policija za objekte in območja SV (ZoBR).

[4] *Protiteroristično delovanje kot eno izmed nalog specialnih sil opredeljujeta Vojaška doktrina (2006: 50) in Direktiva za organiziranje in delovanje specialnih sil SV (2008: 4)*

[5] *Protiuporniško delovanje kot eno izmed oblik specialnega delovanja je v Direktivi za organiziranje in delovanje specialnih sil SV (2008: 4) opredeljeno kot »/.../ podpora protiterorizmu in protiuporništvu (Support to Counterterrorism and Counterinsurgency)«.*

Pri dokončni opredelitvi nalog specialnih sil SV bo zato treba še bolj upoštevati opredelitve v slovenskih normativnih dokumentih ter v MC 437/1 in AJP 3.5. Posebej to velja za **dodatne naloge,** v katerih lahko sodelujejo specialne sile SV. Sodelovanje v njih se določa na podlagi zakonskih pooblastil.

3 TAKTIČNA SKUPINA ZA SPECIALNO DELOVANJE

Vsi koncepti in standardi, ki so uveljavljeni v Slovenski vojski in Natu, se na koncu odrazijo v zmogljivostih. Te zmogljivosti so za posamezne države opredeljene v ciljih sil. Cilji sil SV opredeljujejo, da ESD Natu zagotavlja taktične skupine za specialno delovanje[6] (TSSD). ESD je organizirana tako, da lahko zagotovi več **taktičnih skupin za specialno delovanje**. Nato opredeljuje njihove zmogljivosti in razlike med njimi. Taktična skupina za specialno delovanje iz ESD ima tako element poveljevanja in kontrole, bojni element ter elemente bojne podpore in zagotovitve delovanj. S teh izhodišč so zmogljivosti bojne skupine:

- načrtovanje in izvajanje specialnega delovanja v sovražnih okoljih, samostojno ali kot sestavni del večje formacije, z drugimi vojaškimi in varnostnimi strukturami lastnih ali zavezniških sil ter sil države gostiteljice;
- izvajanje celotnega spektra specialnega delovanja v odvisnosti od posebnih odobritev;
- premeščanje in razmeščanje v načrtovanih časovnih okvirih, z vsemi razredi oskrbe;
- infiltracija in eksfiltracija po kopnem ter po zraku ali vodi;
- izvajanje specialnega delovanja na odročnih območjih in v sovražnih okoljih za daljše obdobje in z minimalno zunanjo podporo;
- izvajanje nalog v podskupinah;
- izvidovanje ter nadzor ciljev podnevi in ponoči, izvajanje nadzora peš in z vozili;
- izvajanje omejenih napadov z daljave z ostrostrelnim orožjem in prenosnimi eksplozivnimi napravami (man-pack explosive devices);
- manevrsko delovanje z uporabo taktičnih prevoznih sredstev in skupinskega orožja za podporo;
- navajanje ter zaključno usmerjanje letalskih napadov ter neposredne zračne podpore;
- navajanje ter zaključno usmerjanje precizno vodenega streliva na cilj;
- razvijanje, organiziranje, usposabljanje in svetovanje oziroma usmerjanje vojaških ali/in paravojaških sil države gostiteljice – z dodanimi prevajalskimi zmogljivostmi.

Zaradi zahtevnosti nalog in razmer, v kakršnih delujejo pripadniki enot za specialno delovanje, sta oprema in oborožitev drugačni kot v drugih enotah. Zaradi različnih načinov in okoliščin delovanja imajo pripadniki specialnih enot več kompletov namenske opreme in oborožitve.

[6] *Special Operations Task Group – SOTG.*

4 KONCEPT »NA UČINKIH TEMELJEČE OPERACIJE«

Koncept »na učinkih temelječe operacije« (UTO) se je na taktični ravni pojavil v zračnih silah ZDA, in sicer v obdobju prve zalivske vojne. Nanaša se na načrtovanje in vodenje bojnega delovanja z združitvijo vojaških in nevojaških metod za doseganje učinka. Razvit je bil za izkoriščanje velikega napredka vojaške tehnologije in razvoja taktike, pri čemer je poveljnikov namen lahko dosežen z minimalno stransko škodo ter minimalnim tveganjem za lastne sile (Batschelet, 2002).

Koncept so pozneje preizkušali tudi na strateški in operativni ravni, vendar so ga zaradi različnih interpretacij ter zaradi mnenja, da daje poveljnikom lažen občutek predvidljivosti bojišča (Mattis 2008), uradno umaknili iz splošne uporabe in ga nadomestili s konceptom »Comprehensive Approach«. Kot govorijo najpomembnejši kritiki, je koncept v primerjavi s tradicionalno operatiko uporaben predvsem z vidika izbire in delovanja na cilje, in sicer na taktični ravni (Vego, 2006; Mattis, 2008; Riper, 2009; glej tudi Smolej, 2011). Tako je, čeprav umaknjen iz uporabe na višjih ravneh poveljevanja, še vedno učinkovito orodje Natovih specialnih sil za določanje ciljev na taktični ravni.

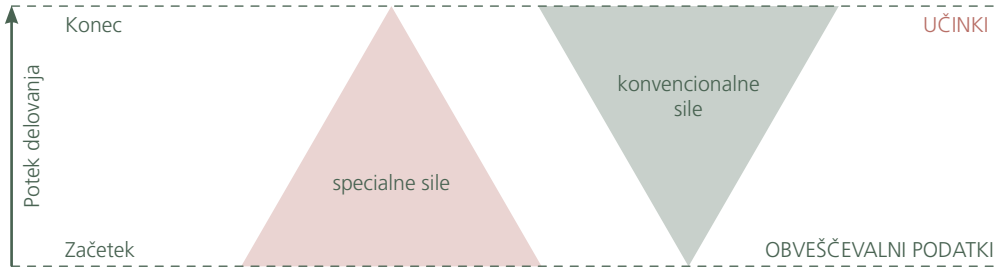
Specialne sile imajo na taktični ravni v bistvu veliko več obveščevalnih informacij o sovražniku kot konvencionalne. To jim omogoča veliko boljši vpogled v stanje na bojišču, saj se konvencionalne sile pogosto na začetku bojnega delovanja znajdejo z omejenim situacijskim zavedanjem. Prav na podlagi večje količine obveščevalnih informacij imajo specialne sile več manevrskega prostora v procesu določanja ciljev, v katerem z uporabo koncepta UTO usmerjajo svoje delovanje v smislu doseganja posebnih učinkov.

Na asimetričnem bojišču to v praksi navadno pomeni, da se poveljniki enot specialnih sil osredotočajo predvsem na cilje, za katere imajo kakovostne in zadostne obveščevalne informacije[7]. Te cilje lahko tudi sami prikrito spremljajo in nadzorujejo (Small footprint) ter v izbranem trenutku z veliko natančnostjo nevtralizirajo. Na drugi strani pa poveljniki nižjih taktičnih enot konvencionalnih sil svoje sile uporabljajo predvsem v smislu prikaza moči (Show the Force), s katerim odvračajo sovražnika od uresničevanja njegovih namer (Big footprint). Če med izvajanjem svojih nalog naletijo na sovražnika[8], poskušajo z njim obdržati stik in ga z okrepitvami uničiti (slika 2).

---

[7] *Menimo sicer, da je lahko tak način pri tako imenovanih anti head operacijah, če je izveden površno, sporen in kontraproduktiven, saj lahko še bolj podžge uporniško delovanje. To se vidi tudi na primeru prenosa strategije generala Petreusa iz Iraka v Afganistan, kjer ni dosegla želenih učinkov (glej tudi Svete, Guštin, Črnčec, 2011).*

[8] *Fizični stik ali obveščevalne informacije.*



Slika 4: Razlika med konceptom delovanja specialnih in konvencionalnih sil

Ko govorimo o učinkih, je treba omeniti predvsem dva vidika, prvi je učinek v taktičnem smislu in je načeloma vezan predvsem na škodo, ki je povzročena sovražniku. Drugi je vezan na operativno raven, in sicer na širše učinke v nekem geografskem in socialnem okolju.

Tako Smith (2006) ugotavlja, da bodo konflikti in spopadi v prihodnje potekali med civilnim prebivalstvom. Glavni akterji konflikta ne bodo države in njihove oborožene sile, temveč različne druge organizirane oblike[9]. Med njimi bo delovanje oboroženih sil po konvencionalnih vojaških načelih povzročilo nepotrebne žrtve in dodaten odpor.

Vojaška operacija je lahko uspešna v taktičnem smislu, vendar je njeno delovanje lahko kontraproduktivno na operativni ravni. To pa pomeni izgubo zaupanja, točke osredotočenja[10] pa niso dosežene.

To se pogosto dogaja v protiuporniškem bojevanju (COIN[11]), v katerem je sovražnikovo delovanje pogojeno predvsem s podporo lokalnega prebivalstva (Celeski, 2005). Tako lahko sicer uspešne vojaške operacije[12] na taktični ravni zaradi stranskih učinkov med civilnim prebivalstvom in na civilni infrastrukturi ali zaradi neodobravanja lokalne skupnosti premaknejo težišče naklonjenosti k sovražniku, kar pa na operativni ravni pomeni veliko več truda in časa za vzpostavitev varnega okolja.

---

[9] *Pri tem se lahko srečamo z mrežno organiziranostjo teroristov/sovražnikov, ki bi jo lahko označili tudi kot organizacijsko asimetrijo. Organizacijska simetrija je bila v zgodovini vojskovanja vedno zelo pomembna. Inovacije so akterjem namreč omogočale veliko prednost, tudi če niso imele tehnološke ali druge prednosti. Tudi Svete (2007, str. 13) trdi, »/.../ da se bodo državne institucije soočile z nedržavnim nasprotnikom, ki bo organiziran v mreže, ne pa hierarhično, kot je organizirana večina državnih institucij na področju nacionalne varnosti«.*

[10] *Teroristi/uporniki delujejo po ljudeh, ki so naša točka osredotočenja (TOS), pri tem ima njihovo taktično delovanje strateški učinek. Točke osredotočenja (angl. Centres of Gravity – COG) so definirane kot značilnosti, zmogljivosti ali prizorišča, iz katerih država, zavezništvo, vojaške sile ali druge skupine črpajo svobodo svojega delovanja, fizično moč ali voljo za boj. Te točke obstajajo na taktični, operativni in strateški ravni in pomenijo središče moči ali delovanja, od katerega je vse odvisno, oziroma so točka, v katero je treba usmeriti vso energijo za doseganje cilja. Iz te točke izhajajo sposobnost, moč in volja nasprotnikovih sil. Uničenje ali onesposobitev te točke pomeni doseganje odločilne prednosti in zmago.*

[11] *COIN – Counter-insurgency.*

[12] *Uspešne v smislu linearnega bojišča, pri čemer je bil cilj predvsem škoditi sovražniku.*

Zato je vodilo bojnega delovanja specialnih sil »razmišljaj operativno, deluj taktično« (Think operational, act tactical). Pri tem je pomembno poudariti, da naj bi specialne sile v protiuporniškem bojevanju v primerjavi s konvencionalnimi, ki izvajajo predvsem kinetične operacije[13] (Smith, 2008), izvajale predvsem nekinetične operacije. To pomeni, da lahko za doseganje svojih ciljev izvajajo naloge psihološkega delovanja, civilno-vojaškega sodelovanja, vojaške pomoči ipd. Tako so specialne sile oboroženih sil ZDA leta 2009 ponovno odkrile koncept Village Stability Operations (VSO), ki je bil v uporabi že med vietnamsko vojno. Glavna značilnost koncepta je, da se manjše skupine specialnih sil nastanijo v ključnih vaseh ali naseljih in v smislu dobrega soseda pomagajo lokalnim skupnostim pri reševanju njihovih težav. Ta pomoč lahko variira od zagotovitve varnega okolja do pomoči pri uvedbi lokalne samouprave[14] in ključne infrastrukture, ki je pomembna za normalno delovanje nekega socialnega okolja. V primeru Afganistana pa je ena izmed ključnih nalog teh specialnih sil zagotovitev povezave lokalne uprave z osrednjo vlado (Government of Islamic Republic of Afghanistan – GIRoA). Glejte že omenjeno knjigo, v kateri je analizirano tudi protiuporniško delovanje okupatorja na slovenskem ozemlju med drugo svetovno vojno.

Koncept UTO je za ESD pomemben, ker glede na svoja izhodišča in druge enote Slovenske vojske narekuje vsebinsko prilagojen proces usposabljanja, ki pa mora biti povezan tako s posamezniki kot tudi z enoto. Za delovanje skladno s konceptom UTO morajo imeti enote specialnih sil veliko večje generične zmožnosti za pridobivanje obveščevalnih podatkov in močnejše analitične zmožnosti za njihovo obdelavo. Poleg tega morajo biti bolj prilagodljive, saj imajo lahko številčno manjše enote specialnih sil veliko večji spekter zmogljivosti, celo v primerjavi večjimi konvencionalnimi enotami. To bi med drugim moralo biti tudi posledica izbirnih postopkov za popolnjevanje teh enot, saj zagotavljajo kadrovsko popolnjenost s sposobnejšim kadrom (glej Spulak, 2007, str. 20).

5 POTRDITEV TEZ IN TAKTIČNA VAJA RIS 2011

Po doktrinarnih in normativnih opredelitvah specialnih sil, njihovi postavitvi in opremljanju, mora vsaka vojska svoje specialne sile tudi preveriti in preizkusiti.

ESD že od leta 2004 deluje v mednarodnih operacijah in na misijah, v katerih SV v praksi preizkuša svoje doktrinarne rešitve. Tako je ESD kot prva v SV opravljala naloge v Afganistanu, Čadu, Libanonu, Iraku itn., znotraj operacij Nata, Evropske unije in OZN.

---

[13] *Termin kinetične operacije (Kinetic Operations) se nanaša na bojno delovanje, pri katerem se uporablja fizična sila.*

[14] *Predvsem v smislu lokalnih varnostnih služb.*

Pri tem je treba poudariti, da naloge ESD v Afganistanu spadajo predvsem med naloge vojaške pomoči (SVNKON 7 Isafa – OMLT[15], NTM-I[16]), delno med izvidniško delovanje (Afganistan SVNKON 1 in 2 Isafa, SVNKON 1 Unifila v Libanonu, SVNKON 1 v Altehei in SVNKON 1 v Čadu). V Afganistanu je ESD opravljala tudi bojno iskanje in reševanje (Afganistan SVNKON 1 in 2 Isafa) in informacijske operacije (INFOOPS, SVNKON 11 Isafa). ESD do zdaj v klasičnih neposrednih akcijah predvsem zaradi vrste nalog, ki jih je sprejela SV, in nacionalnih omejitev ni sodelovala. Kljub dejstvu, da ESD še ni sodelovala v neposrednih akcijah, je pridobila dragocene izkušnje in se dokazala v najzahtevnejših okoljih. Sodobne specialne sile se namreč vse bolj posvečajo nalogam vojaške pomoči in specialnega izvidovanja, kamor spada tudi pridobivanje podatkov s človeškimi viri.

Kot navaja Paternus (2010, str. 64) je operacija Isafa test pripravljenosti in usposobljenosti, ne samo za ESD, temveč tudi za Slovensko vojsko kot celoto, ki je v vojaški operaciji prvič delovala zunaj območja jugovzhodne Evrope. Poleg tega je delovanje v več kot 6000 km oddaljenem puščavskem okolju strokovni izziv in velik logistični dogodek, tako za pripadnike ESD kot tudi za vso Slovensko vojsko. Glede na analizo nalog Natovih enot za specialno delovanje v vojaški operaciji Trajna svoboda (Enduring Freedom) je Paternus (2010) ugotovil primerljivost nalog ESD v Isafu, ki so obsegale:
– globinsko izvidovanje in obveščevalne operacije,
– operacije bojnega iskanja in reševanja,
– iskanje in uničenje skrivališč orožja in streliva,
– urjenje pripadnikov zavezniških sil.

Pridobljene izkušnje iz opravljenih nalog SVNKON 1 in 2 Isafa kažejo na sposobnost ESD za specialno delovanje skladno z Natovimi normativi (AJP 3.5). Glede na zahtevnost nalog in uspešnost pri izvedbi, brez izrednih dogodkov oziroma poškodb, Paternus (2010) ugotavlja, da so pripadniki ESD ustrezno opremljeni, usposobljeni in pripravljeni za specialno delovanje. Njegovo ugotovitev potrjuje tudi delovanje SVNKON 14 in 15 Isafa – OMLT, kamor so vključeni tudi pripadniki ESD.

V operaciji NTM-I so pripadniki ESD z vojaško pomočjo usposabljali pripadnike iraških varnostnih sil. Svoje naloge so opravljali v iraški vojaški akademiji za častnike Al Rustamijah. Pri usposabljanju iraških častnikov so delovali podobno kot pripadniki SVNKON 7 Isafa – OMLT, pri čemer je zagotavljanje varnosti posameznika predstavljalo še večji izziv. Kljub kulturnim razlikam med pripadniki afganistanskih in iraških varnostnih sil so pripadniki ESD dokazali, da so dovolj kulturno osveščeni in sposobni delovati v tujem kulturnem in socialnem okolju, kar je ena temeljnih značilnosti specialnih sil.

---

[15] *Kljub vsem zaslugam SVNKON 14 Isafa, ki je usposabljanje bataljona afganistanske vojske začel leta 2010, je treba poudariti, da je ESD usposabljala afganistansko vojsko že leta 2006. Prav tako so pripadniki ESD usposabljali pripadnike iraške vojske v misiji NTM-I v Iraku leta 2006.*

[16] *NTM – I: NATO Training Mission – Iraq.*

Podobne izkušnje pri delovanju na oddaljenem in zahtevnem puščavskem območju je ESD pridobila v operacijah CAR/Čad in Unifil. Naloge, ki so jih pripadniki opravljali za enote brigadne ravni, spadajo v specialno izvidovanje. Delovali so v lahkih oklepnih vozilih, stopnja samozadostnosti oskrbe je bila velika, kar je bistvena razlika v primerjavi z operacijo Isafa. Velik izziv so bila predvsem terenska vozila, ki morajo imeti v puščavskem okolju večji akcijski radij, medtem ko je zaščita proti improviziranim eksplozivnim napravam (IEN), vsaj v primeru operacije v Čadu, manj pomembna. Obe operaciji, čeprav pod okriljem EU in OZN, sta z vidika opravljenih nalog potrdili koncepte usposabljanja enote. Tudi v teh operacijah so se doktrinarne in konceptualne rešitve, ki izhajajo iz SVS STANAG 2523(1), pokazale kot ustrezne.

Ves obseg nalog (neposredne akcije, specialno izvidovanje in vojaška pomoč), za katerega se ESD usposablja, **se preizkusi na taktičnih vajah**.

Tako se običajno pred pravo bojno uporabo izvedejo usposabljanja in vaje ter tako preizkusijo teoretični koncepti in rešitve. Tudi ESD je svoje konceptualne rešitve ter zmogljivosti za izvedbo bistvenih nalog in poslanstva preverila na taktični vaji RIS 2011.

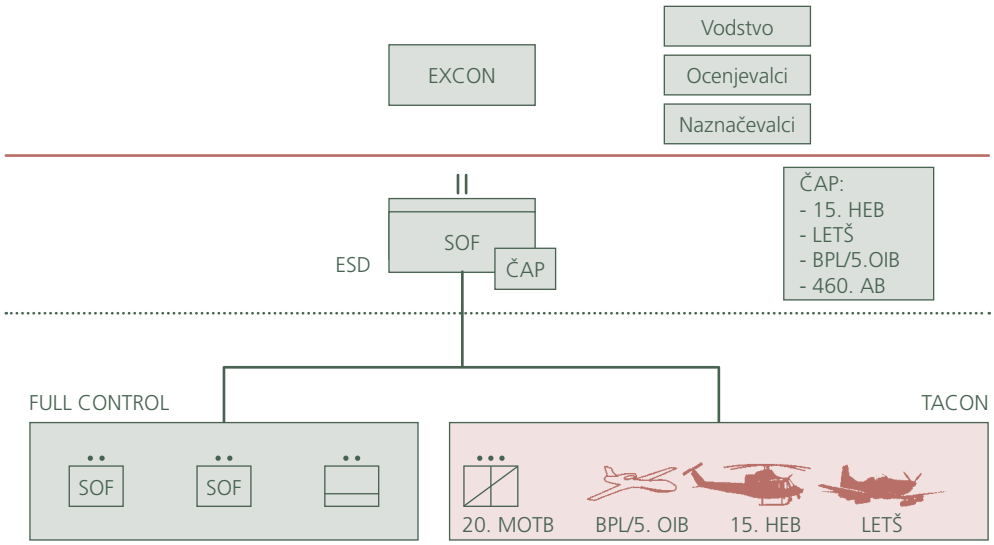
Republika Slovenija se je obvezala, da skladno z načrti razvoja SV v sklopu ciljev sil do leta 2012 razvije in pripravi taktično skupino za specialno delovanje (TSSD), katere nosilec je Enota za specialno delovanje. Za doseganje tega cilja je enota izvedla taktično vajo RIS 2011, katere glavni namen je bil preveriti TSSD pri specialnem delovanju v podporo protiuporništvu (COIN), in sicer v razmerah asimetričnega bojišča, v kakršnem trenutno delujejo enote SV v operaciji International Security Assistance Force (ISAF) v Afganistanu. Hkrati je ESD želela preveriti zmožnost TSSD za izvajanje združenega bojevanja rodov, saj to zagotavlja sinergične učinke (1 + 1 = 3), ki specialnim silam omogočajo relativno premoč[17] v prostoru in času nad številčno močnejšim sovražnikom. Na vaji so sodelovale enote sil SV (slika 5):

- ESD z elementi:
  - poveljstvo z izvajanjem nalog poveljevanja in kontrole (PINK),
  - bojne skupine, ki so izvajale kinetične operacije (DA) in vojaško pomoč (MA) v povezavi s konvencionalnimi silami države gostiteljice (HN) ter pridobivale in potrjevale obveščevalne informacije – specialno izvidništvo (SR),
  - logistična skupina (LOGSK) za bojno zagotovitev delovanja;
- Letalska šola (LETŠ) z zrakoplovi PC-9M Hudournik za ognjeno podporo iz zraka;
- 15. helikopterski bataljon (HEB) za zagotovitev zračne premičnosti;
- 5. obveščevalno-izvidniški bataljon (OIB) s skupino brezpilotnih letal (BPL) za zagotovitev obveščevalnih podatkov – slikovnega gradiva (IMINT[18]) ter za nadzor ciljev;
- 460. artilerijski bataljon (AB) za topniško podporo;
- 20. motorizirani bataljon (MOTB) z izvidniškim vodom (IZVOD), ki je opravljal naloge sil države gostiteljice.

[17] *Relative Superiority (McRaven, 1995).*

[18] *IMINT– Image Intelligence.*

Slika 5:
Organizacija sil vadbenih elementov za vajo RIS 2011



ESD je za stvarno preverjanje odzivnosti in delovanja enote načrtovala izvedbo vaje po načelu klasičnega delovanja v mednarodnih operacijah in na misijah (MOM), in sicer na vadbeni situaciji Afganistana.

Glede na vadbeno situacijo je dobila nalogo poiskati in v sodelovanju s silami države gostiteljice zajeti osebo oziroma cilj visoke vrednosti. Z izvedbo naloge naj bi pridobila nove obveščevalne podatke, s katerimi bi onemogočila delovanje sovražnikove mreže, hkrati pa bi prikazala zmožnost in zanesljivost osrednje afganistanske vlade – GIRoA[19], da zagotavlja suverenost v določeni provinci.

V prvem delu vaje je enota skupaj s skupino BPL vadila pridobivanje obveščevalnih podatkov na območjih posebnega interesa (NAI[20]). Po obveščevalni analizi slikovnega gradiva (IMINT) je na podlagi teh informacij opravila še proces premišljenega odločanja po modelu *Military Decision Making Process* in skladno z odobreno varianto delovanja izdala naloge podrejenim enotam. Hkrati je na dislocirani lokaciji bojna skupina izvedla usposabljanje voda države gostiteljice in tako ustvarila razmere za skupno združeno (Combined Joint) bojno delovanje.

V nadaljevanju vaje se je bojna skupina, razdeljena na dve podskupini, ob zračni podpori premaknila na dve ločeni ciljni interesni območji (TAI[21]) in zagotovila njuno opazovanje ter nadzor. V nadaljevanju je ena podskupina opravila pozitivno identifikacijo iskane osebe, medtem ko je druga locirala in identificirala osebo z združene

[19] *GIRoA – Government of Islamic Republic of Afghanistan.*

[20] *NAI – Named Area of Interest.*

[21] *TAI – Target Area of Interest.*

liste iskanih oseb (JPETL[22]). Po predaji slikovnega gradiva poveljstvu ESD je to potrdilo pozitivno identifikacijo ciljev in se na podlagi štabne analize odločilo, da iskano osebo zajame z združeno enoto lastnih sil in sil države gostiteljice, medtem ko drugi cilj visoke vrednosti zaradi njegovega profila in zaradi omejenih lastnih bojnih zmogljivosti uniči z letalskim ognjem.

Na prvem ciljnem interesnem območju je podskupina s pomočjo para letal PC-9M Hudournik z letalskim ognjem uničila cilj. Uničenje cilja brez stranske škode je pozneje potrdilo tudi slikovno gradivo, ki ga je za oceno bojne škode posnela skupina BPL. Istočasno je na drugi, oddaljeni geografski lokaciji združena enota opravila premik na drugo ciljno interesno območje in zajela iskano osebo. Po zajetju je na kraju dogodka zbrala in zavarovala obremenilne dokaze (SSE[23]), ki jih je pozneje skupaj z zajeto osebo predala poveljstvu ESD. Poveljstvo je izvedlo vse nadaljnje predvidene postopke.

Sklep

Tako v mednarodnih operacijah in na misijah kot na taktični vaji RIS 2011 je ESD pokazala, da je vrhunsko usposobljena enota, ki tvori ost enot za bojno delovanje Slovenske vojske. Enota je doslej v praksi in na vaji preverila in potrdila zmogljivost **specialnega delovanja** ter **združenega bojevanja rodov** v podporo nalogam protiuporništva (COIN), in sicer v razmerah asimetričnega bojišča, na kakršnem trenutno delujejo enote SV v operaciji Isafa. S potrditvijo svojih zmogljivosti v praksi je ESD pokazala, da so predlagani teoretični koncepti in rešitve, na katerih temelji, pravilni in uresničljivi. S tem je ponovno potrdila svojo zavezanost k odličnosti in preseganju standardov. Ponovno so se potrdili reki, da je kakovost pomembnejša od količine, da je človek s svojim znanjem in izkušnjami pomembnejši od opreme, pa tudi, da pripadnikov specialnih sil ni mogoče usposobiti na hitro, tudi če je nuja.

Za dokončno umestitev med specialne sile in za specialno delovanje v Natu, v resnični operaciji, je treba določiti tudi vodilno državo (Leading Nation), kar pa ni v pristojnosti ESD.

Sistemski in celovit pristop k oblikovanju ESD zagotavlja zmogljivost specialnega delovanja Slovenske vojske in posebnih nacionalnovarnostnih ciljev Republike Slovenije. Usposabljanje in opremljanje enot za specialno delovanje je dolgotrajen proces, ki mu morata država in vojska nameniti dovolj pozornosti (tudi kadrovskih in materialnih virov).

Visoka usposobljenost, sposobnost prikritega delovanja, zmožnost velike natančnosti zaradi zmanjševanja stranskih učinkov in velika prilagodljivost glede na različne vire ogrožanja so samo nekatere značilnosti, ki poudarjajo vlogo in pomen ESD znotraj oboroženih sil. Te značilnosti omogočajo njeno uporabo za izpolnjevanje obveznosti Republike Slovenije do sistema Natove kolektivne obrambe ter

[22] *JPETL – Joint Priority Enemy Target List.*

[23] *SSE – Sensitive Site Exploitation.*

zagotavljanje mednarodne varnosti v mednarodnih operacijah in na misijah znotraj OZN, ko drugih enot in zmogljivosti Slovenske vojske ni mogoče uporabiti. Hkrati pa Republika Slovenija pridobi tudi zmogljivosti za obrambo države in delovanje v posebnih kriznih razmerah[24] protiterorističnega delovanja v Republiki Sloveniji.

Literatura

1. *AJP-3.5. Združena zavezniška doktrina specialnih operacij (izvirnik januar 2009, slovenski SVS STANAG 2523(1), julij 2009). Ljubljana: MO RS.*
2. *Batschelet, A. W., 2002. Effects-based operations: A new Operational Model? Strategy Research Project, U.S. Army War College. http://www.iwar.org.uk/military/resources/effect-based-ops/ebo.pdf, 5. 5. 2011.*
3. *Beršnak, K., 2010. Preoblikovanje vloge in načinov delovanja enot za specialno delovanje zveze Nato v povezavi z evolucijo tipologije vojskovanja. Diplomsko delo, Maribor: Fakulteta za varnostne vede.*
4. *Celeski, J, D., 2005. Operationalizing COIN. Joint Special Operations University (JSOU) Report 05-2.*
5. *Furlan, B., in drugi, 2006. Vojaška doktrina. Ljubljana: Defensor.*
6. *Mattis, J. N., 2008. USJFCOM Commander's Guidance for Effects-based Operations. Parameters, Vol. XXXVIII, pomlad 2008. str. 18–25. http://www.carlisle.army.mil/usawc/Parameters/Articles/08autumn/mattis.pdf, 9. 6. 2010.*
7. *Newton, R., 2010. Introduction to Special Operations. What makes SOF special. PP-predstavitev, Chievres: NATO SOF.*
8. *Paternus, U., 2010. Preoblikovanje vojaških specialnih enot držav zveze NATO. Magistrsko delo, Ljubljana: Fakulteta za družbene vede.*
9. *Prezelj, I.,2007. Nujnost medresorskega sodelovanja in koordiniranja v boju proti terorizmu: nekateri primeri iz Republike Slovenije. V: Bilten Slovenske vojske 2007-9/št. 2. Ljubljana: Generalštab Slovenske vojske, str. 65–80.*
10. *Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2025 (ReSDPRO SV 2025), 2010. Uradni list R, št. 99/2010 z dne 7. 12. 2010.*
11. *Riper, K. P., 2009. EBO There Was No Baby in the Bathwater. Joint Force Quaterly Issue 52, str. 82–85.*
12. *Rode, A., 2007. Vojaška obveščevalna dejavnost. Magistrsko delo. Celje: Fakulteta za logistiko.*
13. *Smith, H., 2008. Kinetic and Nonkinetic Versus Lethal and Nonlethal Operations.*
14. *http://www.captainsjournal.com/2008/06/30/kinetic-and-nonkinetic-versus-lethal-and-nonlethal-operations/*
15. *Smith, R., 2006. The Utility of Force. The Art of War in the Modern World. London: Penguin Books.*
16. *Smolej, S., 2011. Kritična analiza na učinku temelječih operacij. Magistrsko delo, Ljubljana: Fakulteta za družbene vede.*
17. *Srednjeročni obrambni program 2007–2012 (SOPR), št. 803-2/2006-58 z dne 27. 11. 2006.*
18. *Spulak, R., 2007. A Theory of Special Operations. Joint Special Operations University (JSOU) Report 07-7. http://jsoupublic.socom.mil/publications/jsou/JSOU07-7spulakATheoryofSpecialOps_final.pdf, 4. 6. 2010.*
19. *Svete, U., 2007. Asimetrični konflikti in mirovne operacije. Polječe, Center za obrambno usposabljanje. 19. 11. 2007.*

[24] *Uporaba vojaških zmožnosti bojnega delovanja ob razglasitvi izrednih razmer.*

20. *Svete, U., in drugi, 2011. Asimetrija in nacionalna varnost: od zgodovinskih izkušenj do sodobnih izzivov. Knjižnica Jurija Vege. Ljubljana: Defensor.*
21. *Vego, N. M., 2006. Effects-Based Operations: A Critique. Joint Force Quaterly Issue 41, str. 51–75.*

http://www.slovenskavojska.si/publikacije/sodobni-vojaski-izzivi/
http://www.slovenskavojska.si/en/publications/contemporary-military-challenges/

Vsebina