AARMS Vol. 12, No. 2 (2013) 329–342. **10.32565/aarms.2013.2.14**

Small Countries and Cyber Defence

SHERIFI, Shkendije, G.[1], NAGY Károly[2]

Cyber security problems pose a particularly important challenge for Small Coun- tries. Their achievements can easily be destroyed by a cyber attack. Therefore, Small Countries cannot rely on the great powers or alliance systems the same way they would in the case of a military threat. A new interpretation of the concept of cyber space creates a new approach to cyber security problems. This new approach and the cooperation with the cyber defence system of NATO facilitate the development of an individual cyber security policy and the support of social development.
Key words: cyberspace, virtual worlds, cyber security, cyber defence, comprehen- sive approach

Introduction

Cyber security problems are now in the focus of the security efforts of the great powers and international institutions. It is particularly difficult for the so called Small Countries to find a solution to these problems. The expression Small Countries is used for countries which are unable to ensure the realization of one or more basic state functions. Such basic functions are the guarantee of the sovereignty and territorial integrity of the country; providing public edu- cation, public services such as law and order etc. The above would imply that small countries are aid economies; but this is not the case. It is true that all aid economies can be regarded as small countries, but countries which need the help of the great powers or an alliance system to ensure their sovereignty or territorial integrity are not necessarily aid economies. There have been other reasons for the introduction of the rather fuzzy definition of small countries as well. We do not want to use the expression aid economy due to our critical view of current international aid delivery processes.[3]

1 National University of Public Service, Budapest Hungary, Shkendije Geci Sherifi, shkendije.geci@gmail.com
2 Protan Information Security Consulting Services Company, Budapest, Hungary
3 We have introduced our criticism and discussed the opportunities to be exploited in our study. (Nagy, Karasszon, 2008) Unexploited opportunities result from the fact that aid economies do not have deep rooted institutions; therefore, an institutional system and virtual economic zones based on the latest Information
and Communication technology (ICT) developments could easily be established to meet the challenges
of globalization. Unfortunately, this is not happening. Donor countries often use aid economies as a dump for their obsolete technology. Opportunities inherent in aid economies to facilitate the development of globalization remain unexploited.

According to the above definition Afghanistan[4] or the considerably smaller Kosovo[5] can both be regarded as SCs. It should be noted that the present study does not discuss the possi- ble SCs. Some specific examples with regard to Kosovo and Afghanistan are only provided to facilitate the better understanding of our argument.

This condition raises special issues with regard to the organization of the defence and security of SCs. We are convinced that there is more at stake than the seemingly negligible local problems of SCs. Due to the global connection of info-communication systems, cyber criminals and cyber terrorists can penetrate these countries, even if only virtually, similarly to al–Qaeda in Afghanistan. If that happens, these centres pose a global threat.

The deterrent force of the great powers, the International Community, or an alliance sys- tem is able to provide effective defence against armed interventions directed at SCs. De- terrence is based on possible retaliation and/or on rapid reaction, which renders the attack futile from the very beginning. But is it the same in the case of a cyber attack? Apparently not, or not exactly. Assistance may be provided, but what kind of retaliation could be used for deterrence when often it is not even clear who the attacker is, let alone providing evi- dence for state level intervention?[6] Cyber attacks are often carried out under a foreign banner through the use of unconventional forces, such as multiple hacker communities[7]. In spite of the disproportionately greater capacities of external defence forces, how could collaboration be possible on an equal footing? Such questions can be answered on the basis of an effective cyber security policy. The objective of our research is to provide a general theoretical and methodological model for the cyber security policy of SCs.

4 According to the NATO Secretary General, by 2014 Afghanistan will be able to guarantee its own security: "*Our current combat mission will be completed by the end of 2014, when our Afghan partners have assumed full responsibility for the security of their country*". (NATO, 2012a) Accordingly, Afghanistan – if it does not need long term external aid in any other respect- will cease to be a Small Country by our "working definition"

5 There is another situation with Kosovo. The security umbrella of Kosovo is becoming stronger. On one hand, "*the Secretary General made it clear that NATO and KFOR will continue to guarantee security in Kosovo and remain ready to deal with any attempts to undermine the progress that has been made*". (NATO, 2013a) On
the other hand, Camp Bondsteel is carrying out IT developments which might have cyber security aspects as well: "General Dynamics will provide information technology (IT) support to USAREUR headquarters and its associated staff elements and organizations as part of the USAREUR Theatre Warfighter Command, Control, Communications, Computers and Intelligence (C4I) program. The majority of work will be performed at the USAREUR headquarters in Heidelberg, Germany, at other sites within Germany and at Camp Bondsteel, Kosovo". (NATO, 2013a)

6 NATO holds the following view: "*Furthermore, there is virtually no effective deterrence in cyber warfare since even identifying the attacker is extremely difficult and, adhering to international law, probably nearly impossible. Under these circumstances, any form of military retaliation would be highly problematic, in both legal and political terms*". (NATO, 2011) Some experts believe that such cyber weapons as the Stuxnet fire- and-forget weapon could be used as a deterrent, for they can cause physical damage through a simple data (code) flow. (Lee, 2012) In our opinion, such deterrence is a double edged sword, for "*conceptually location can be grasped as a meeting point, an inter-crossing point of activity fields, connections and vital relations, influences and movements*". (Castells, 1996: 356)

7 According to J. Davis, "*What is worrying in this regard is the potential nexus between state-sponsored attacks against NATO and non-state armed groups that might be tasked to carry out such an attack… In the cyber arena, there is also the possibility of non-state actor attacks, sponsored by a nation-state, as seems to be the case with recent probes into US and NATO security networks*." (Davis, 2011)

Cyber Security Climate Change

Several factors indicate that a different approach is required to reduce the cyber security problems of Small Countries to a manageable level. The priorities of Small Countries should also be determined correctly for them to be able to join international collaboration processes.

Signs of threat

In 2009—2010, a serial was published on the possible consequences of a large scale attack against the United States, referring to an "*Information Digital Pearl Harbour"*[8]. Such warn- ings are endless. However, relevant NATO statements indicate that they should be taken seriously. (NATO, 2011)

With regard to the most important conditions of defence, a Hungarian study has also been published. (Kovács, Krasznay, 2010) The authors, Kovács and Krasznay, illustrate the threats to the national economy and political system in case of a cyber attack. The magnitude of damage is compared to the biggest tragedy in Hungarian history: the lost battle against the Ottoman Empire at Mohács on 29 August 1526.

In the Introduction by the Rt Hon Francis Maude MP, Minister for the Cabinet Office of the UK Cyber Security Strategy (Cabinet Office, 2011) he wrote: *"the 2010 National Secu- rity Strategy rated cyber attacks as a 'Tier 1' threat and why, despite a tight fiscal situation, we set £650 million aside over four years to develop our response."* If cyber attacks are the
'Tier 1' threat' for the UK, it must be the same for SCs, too. However, SCs do not even have a chance to finance their cyber security activities at a level reaching a critical mass.

Cyber security problems have become more serious since the above warnings. For ex- ample, Kaspersky holds that "the world needs to come to an agreement over cyber weapons just like it has with nuclear and biological weapons" (Parrish, 2012) In July this year, at the G8 summit a US Russian agreement was made about the establishment of a cyber hotline to prevent accidental cyber war. (Gallagher, 2013)

According to our research results, there is a solution for SCs to take effective measures to guarantee their own security and sovereignty and exploit the opportunities which are de- scribed in the UK Cyber Security Strategy as follows: "*Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society"* (Cabinet Office, 2011)

For the efforts of SCs to be successful, positive changes are required in the world. Since SCs cannot do too much to influence the above, it can be regarded as a kind of climate change. Individual countries must adjust to these changes, the development of which can be influenced through global cooperation.

8 Such work is the study of Dominic Basulto (2010), or paper (Letter from the Capitol, 2010).

Cyberspace

The theatre of cyber war, envisioned by many, is cyberspace. Despite this approach, we agree with the view held by Libiczki: "*Understanding cyberspace as a warfighting domain is not helpful when it comes to understanding what can and should be done to defend and attack networked systems. To the extent that such a characterization leads strategists and operators to presumptions or conclusions that are not derived from observation and experience, this characterization may well mislead.*" (2012: 322)

For example, the UK Cyber Security Strategy uses the following definition: "*Cyberspace is an interactive domain made up of digital networks that is used to store, modify and com- municate information. It includes the internet, but also the other information systems, that support our businesses, infrastructure and services."* (Cabinet Office, 2011: 11) As we can recognize here cyber space is no longer referred to as a "warfighting domain".

We start out from our earlier defined concept, which is the following: "*The "medium" carrying the structures of the information society is cyberspace. Cyberspace is the rapidly widening universe of the virtual worlds. We can join cyberspace via local virtual worlds. Cy- berspace technology connects the functions of the computer with the abilities of the human…. The age of the information society will arrive when the virtual worlds created by human imagination will be reified on the basis of the achievements of electronic technology, and the participation of people in these virtual worlds becomes wide–spread, general and routine.*" (Nagy, 2001: 107)

According to this approach, the development of society points towards the creation of a global information society. Consequently, in the long run cyber security becomes a central issue for participants joining the virtual worlds. "*A person joining a virtual world is exposed to a considerable number of dangers ranging from a violation of basic human rights to imme- diate physical or neurological damage. Therefore the operation of virtual worlds involving wide masses requires social conditions in which human and personal rights enjoy a higher protection than they every did before*." (Nagy, 1996:151) That is the reason why not much is said about the information society these days. Following 9/11, the development of the infor- mation society came to a halt. (Nagy, 2007a: 49)

While approaching the concept of cyberspace from the aspect of virtual worlds might seem utopian, a new challenge to our imagination and problem solving capacities has al- ready emerged. Founded by Russian entrepreneur Dmitry Itskov in February 2011, the proj- ect "*The 2045 Initiative"* aims to create technologies enabling the transfer of an individual's personality to a more advanced non–biological carrier, and extending life to the point of immortality. (Itskov, 2012) The project *The 2045 Initiative* also forecasts the emergence of new dimensions of future, or so called virtual needs in the field of cyber security. It is not yet certain whether this initiative will ever be implemented, but from the point of view of strategic thought development it would be useful to analyse it in depth, through a scientific approach, as to what new challenges we might have to face to ensure the undisrupted survival of the human mind on a technological basis without any mutations. The importance of the above — as discussed by Szab*ó* in detail (1985: 329) — is that if we can satisfy certain future or virtual needs in the present, then some unsatisfied present or effective needs will automat- ically disappear. Consequently, this kind of strategic view facilitates the effective solution of both present day and future problems.

SHERIFI, Shkendije, G., NAGY Károly: Small Countries and Cyber Defence

A new approach is required

If we consider that the health and lives of people participating in virtual worlds is threatened by cyber security problems, then the interpretation of Kovács and Krasznay seems to lose its validity: "*By attacking information technology systems no losses or only indirect losses are caused in human lives, but the economic and political damages are insurmountable.*" (Kovács, Krasznay, 2010: 45)

In the future the health and lives of people will be directly threatened by cyber security problems, which will eventuate a new view of these problems. The most serious result could be the classification of cyber weapons as weapons of mass destruction. In the virtual worlds they can disrupt the functioning of technological systems and cause health problems. Accord- ingly, Kaspersky's recommendation might be reconsidered in the field of the non–prolifera- tion of weapons of mass destruction.

In the field of information and information–communication technology (I/ICT) security, often the most fundamental things are optional. If a car does not meet the relevant techni- cal requirements and specifications in force, it cannot be used in traffic. On the other hand if someone wants to install a fire–wall on their computer, they can do so, but they are not obliged to do so. At the same time, if a computer without sufficient protection is used on the internet, it poses a potential threat to other users as well. In summary the security in ICT systems cannot be optional. Every ICT system must meet internationally set security require- ments at production and installation[9].

1. Changes are required in the following five areas to reduce the complexity of the cyber security problems of Small Countries to a manageable level:
2. Similarly to the prevention of the proliferation of weapons of mass destruction, an inter- national surveillance and

control system should be established to prevent the develop- ment, production and use of cyber weapons;
3. Security in ICT systems cannot be optional. Every ICT system must meet internationally set security requirements at production and installation;
4. The use of backdoors should be banned by international agreements, and the authoriza- tion of exceptional cases should be strictly regulated;[10]
5. The responsibilities of telecommunication, cloud and other service providers concerning the data they receive should be established by international agreements. There should be clear regulations with regard to the provision of data to a third party without the authori- zation of the client, and the responsibilities for the resulting damages;
6. In the field of privacy protection, efforts directed at the widespread application of digital signature and of secure digital codenames should be renewed and supported.[11]

9 One of the objectives of NATO is to develop such a requirement system. (NATO, 2013b) This could be adopted by Small Countries as well, even if they are not NATO members.

10 One of the authors of the present study points out the dangers related to the use of back doors in his former work. (Nojeim, 2012) Nojeim calls efforts directed at the use of back doors and similar applications "backfire policy". (Chaum, 1992: 426)

11 There were cryptographic applications in the 1990s that provided strong protection in the field of privacy. For example, cryptographic invention known as a "blind signature" was published in 1992. (Kovács, 2009) The importance of the application of cryptographic protocols was pointed out by us in the following publication (Nagy, 1996) (Nojeim, 2012)

In order to achieve success in c, d, and e, the great powers should deal with "problematic cyber security policies", or "backfire policies" in their own countries.

Problematic Cybersecurity Policy Ideas

According to Nojeim "*Washington is awash with cyber security policy ideas for Congress to choose among. Some policies are "low hanging fruit" that should have been adopted long ago. But others, including those outlined in this article, could do more harm than good by un- dermining civil liberties and necessary information sharing, slowing down decision making and moving decision–making authority from the best decision makers, and creating perverse incentives and unexpected economic and systematic impacts, all of which would undermine cyber security.*" (Chaum, 1992: 432)

The paper of Nojeim identifies some of the most problematic cyber security policy ideas, explains how they could backfire, and offers in each case an alternative approach that could accomplish the goals of the policy proposal called into question. It explores proposals to:

- empower the government to block or limit Internet communications on private networks;
- give the Department of Defense the lead cyber security role for civilian government and privately owned critical infrastructure information systems;
- have the government monitor private networks and communications for cyber security reasons; and
- increase the scope of what is lawful electronic surveillance by re–architecting new com- munications technologies and services to make them more wiretap ready.

Each of these proposals would unjustifiably increase the federal government's ability to take unilateral action in networks otherwise (and more appropriately) subject to highly distributed governance. According to Nojeim, SCs might be affected by the "Internet Kill Switch" proposal (Chaum, 1992: 409), the "On–Going Information Sharing as a Back–Door to Governmental Monitoring" (Chaum, 1992: 426) and the "Impose Design Mandates on New Communications Technologies to Facilitate Electronic Surveillance" (Chaum, 1992: 429) initiative. Due to the global economic role of the US, the internet Kill Switch might have tragic consequences for SCs because the internet economy would become dysfunc- tional. The other two, as Nojeim points out, "*could backfire by discouraging the growth of technologies, such as cloud computing, that rely on the privacy of communications*" (Chaum, 1992: 427) and "*can also undermine security because such a database could, itself, become a target for hackers.*" (Chaum, 1992: 428)

Cyber Defence

Let us assume that due to a positive cyber security climate change there is a chance for SCs to improve their security situation. To make these efforts more effective, they should take part within the framework of international cooperation. Such a framework is offered by NATO. Following the introduction of that framework, our suggestions with regard to priorities are made accordingly.

NATO Cyber Defence

In the present study, as opposed to the concept of cyber security, the concept of cyber defence is not used in general. Instead, we want to refer to the relationship between SCs and NATO Cyber Defence. NATO Cyber Defence is not a reincarnation of information warfare within the framework of NATO[12]. These two concepts significantly defer from each other, especially since information warfare is not only defensive in nature.

NATO Cyber Defence is a complex system of collaboration, doctrines, theories and vari- ous processes required for the implementation of NATO's Cyber Defence policy. The expres- sion NATO Cyber Defence refers to the totality of the activities of NATO carried out in the interest of cyber security. NATO Cyber Defence is not a model for SCs. SCs should not create a small cyber defence. Instead, they should participate in the cyber security activities of the Alliance. Small Countries should develop and implement their own cyber security policy.

According to NATO Cyber Defence Policy, "NATO's top priority on cyber defence is protecting the communication systems owned and operated by the Alliance. The protection of rational critical infrastructures remains a national responsibility, which requires nations to invest resources in developing their own capabilities. NATO is helping Allies in their efforts to build up cyber defences by sharing information and best practices and conducting cyber defence exercises." (NATO, 2013b) An important source for SCs to create their own critical infrastructure cybersecurity protection plan is the "Executive Order — Improving Critical Infrastructure Cybersecurity". (The White House, 2013)

At the same time it is apparent that NATO integrates the problem of cyber security into a unified system in the name of a comprehensive approach with other areas of defence and security[13]. NATO has developed a wide ranging global collaboration[14] where the organization of collective work has an important role in dealing with cyber security problems. NATO has also established close cooperation with the private sector and the world of academia. The integration of SCs into the Cyber Defence Policy system of NATO will have the following advantages:

- Use of best practice;
- Education and training;

12 In his study "Electronic Warfare and the Asymmetric Challenge" Kovács points out that "*information warfare as a term was removed from doctrines in the US and from NATO's documents as well in early 2000.*" (Kovács, 2009: 137) The term information warfare also included electronic warfare. At the same time, as a result of developments and conceptual changes, Libiczki says the following: "*Things did change. The term information warfare, in the process of morphing into "information operations," created "influence operations," which covers psychological operations and concomitants, such as strategic communications. The cyber part of this formulation, computer network operations, married the "cyber" prefix and separated itself completely from matters psychological. Electronic warfare returned to its own aerie. So, at least the term, information warfare, has been rectified.*" (2012: 336)

13 "*However, in today's world, territorial defense must embrace critical infrastructure protection, consequence management, planning to thwart an Electro-Magnetic Pulse (EMP) attack, aspects of energy security and cyber operations*". (Davis, 2011)

14 The latest news, that NATO and Colombia signed an Agreement on the Security of Information, is an accord that will allow NATO and Colombia to explore future cooperation and consultation in areas of common interest. The Security of Information Agreement does not formally recognise Colombia as a NATO partner but constitutes a first step for future cooperation in the security field. It will facilitate the participation of Colombia in a number of NATO activities. (NATO, 2013c) The first step in NATO—SCs collaboration should be the conclusion of such an agreement.

- Comprehensive approach;
- Security requirements based on wide ranging collaboration;[15]
- Large scale international collaboration.

The "cyber defence approach" has an additional advantage: even if only implicitly (as we mentioned in the footnote 9), due to its military aspects, it opens a door to electronic warfare, without the knowledge with which any successful cyber security activities are possible. We use the word implicit because the place of electronic warfare has shifted significantly in re- cent years, and although it seems steadier nowadays, it is not yet been recognized in public NATO documents.

In other words, the Cyber Defence System of NATO is based on consensus, it is clear and offers a global framework for Small Countries within which they can implement their own cyber security policy effectively.

Smart ICT Developments

Advances in ICT (Information and Communication Technology) such as Cloud Computing and Big Data Applications offer further opportunities to reduce the complexity of cyber se- curity problems.

Cloud is a resilient, distributed parameter system. It hides the target from the eyes of the attacker. The defence of Global Cloud will be established through a global effort. Instead of defenceless and divided users, cyber criminals will have to face gigantic multinational service providers with vast resources. In the cyber security activities of countries emphasis from the control of their own citizens should be shifted to the control of these big service providers.

Cloud Computing and Big Data applications make it possible for SCs to spread their cyber security risks, create new conditions to ensure the authenticity of information, and eliminate unreasonable objections to processes facilitating social development.

In the development of the ICT infrastructure of Small Countries cloud applications have one more important advantage: Small Countries do not get involved in futile and anachronis- tic hardware and software developments (it is like trying to develop and manufacture a car on your own); instead, they can use their resources to develop user creativity.[16]

Cyber Security Knowledge Centre

The study "The Role of Knowledge Centres in Information Warfare" illustrated that the most effective defence in information warfare waged with the assistance of state institutions can, paradoxically, be provided by the network of institutions under civil control; that is, by knowledge centres. (Nagy, 2007b) Nagy, K. (2007) The concept of knowledge centres

15 "*NATO will identify its critical dependencies on the Allies' national information systems and networks and will work with Allies to develop common minimum security requirements."* (NATO, 2013b)

16 Kosovo could be a nice example for the potential of this creativity: "*Kosovo Digital Diplomacy Strategy reviewed as one of the best in Europe*". (Kosovo's New Diplomat, 2013)

has various definitions, and implementations[17]. We can define the concept of cyber securi- ty knowledge centres through the following basic functions. These functions illustrate that the Cyber Security Knowledge Centre is different from NATO Cooperative Cyber Defence Centre of Excellence (Nagy, 2009b) and it is different from Computer Emergency Response Teams (CERTs), too.

Developing a new security culture is an essential pre–condition for exploiting the oppor- tunities offered by a network of knowledge centres. (NATO CCD COE)

The functions of the Cyber Security Knowledge Centre (CSKC) are as follows:

1. Fast and efficient output of new knowledge and information required for competent cy- ber security related policy–making, developments, etc.;
2. Acceleration of the acquisition of practical knowledge required for competent cyber se- curity related policy–making, implementation of policy guidelines and for the identifica- tion of specific problems arising in connection with cyber security;
3. Creation, maintenance and continuous improvement of a platform designed for the effi- cient transfer of knowledge; establishment of foundations with completely new charac- teristics, to be used in addressing cyber security issues in order to provide best practice methodology.

New Security Culture

In order to gain public support and strengthen the development of social capital, security culture programs should be established. An example for that is the "New Security Culture Programme" launched in Hungary in 2007. (Nagy, 2007c)

The first step for Hungary in the establishment of the New Security Culture Programme was a lecture called "Security of virtual worlds." (Nagy, 1996)[18] The context of this lecture provided the opportunity to present some aspects of the cornerstones of cyberspace secu- rity philosophy. The definition below has become the basic principle for cooperation, also included in the motto of the New Culture of Security Programme (Culture of Cooperation – Cooperation of Cultures): "*The relationship between the "participants" in the cyberspace and the institutions should be one where unilateral control and confrontation is replaced by cooperation based on mutual trust. In order for this precondition to become implementable re- ality, instead of hopeless and ineffective attempts aimed to control cyberspace communication, institutional resources should be shifted towards cooperation with participating communities and the exploration, localisation and elimination of "black holes*" (coalitions with a non–pub- lic distribution technique used for the manifestation of partial interests)". (Nagy, 1996: 154)

This basic principle was later confirmed by a pertinent OECD initiative with the "force of harmony" (OECD, 2002), a UNO decision based on this (UN General Assembly, 2004) and the "Act on Cyber Crime" (Cornell University Law School, 2002), an act which was passed in the USA in 2002. It should be noted that the OECD initiative advocates the creation of a new culture of security mainly in order to address cyber security problems.

17 Since then, the concept of knowledge centres of similar functionality has been developed for energy security centres. (Nagy, 2009a) The theoretical and methodological background required for the creation of virtual knowledge centres has been published in a renowned scientific journal (Nagy, Körmendi, 2012), and the technological conditions have been developed. (Nagy, 2009b) As a result, they can be established any time.

18 This initiative had another significant scientific background in the work of the co-authors Várhegyi and Makkay too. (2000: 199–206)

The procreation and the operation of a security culture program require an extensive international cooperation. Its essential part is the cooperation on scientific and technological fields. The above mentioned "NATO framework"

provides excellent conditions for the SCs to develop their own security culture programs.

Privacy

The most difficult task presented is fighting resistance to finding solutions for the protection of privacy. Providing privacy is a social task and it is a basic requirement for the creation of social capital. The protection of privacy is a key issue in democratic legislation and it is the fo- cal point of security culture. Providing privacy requires time and sufficient financial resourc- es. It is important to look at the problem of privacy in a historical context. (Peterman, 1993)

We have arrived at the conclusion that due to the complexity and global impacts of the question, there is only one viable solution for SCs: They should adopt practices used in de- veloped democracies, such as the United States. [19] Privacy and human rights may be restricted for security reasons just like in the US[20], but only if SCs can offer the same guarantees as the US. If these guarantees do not exist, privacy should enjoy a priority.

The situation with the privacy in Kosovo is an example, that despite the difficulties these problems could be solved at the highest level: "Over the five past years, Kosovo has made remarkable progress, institutions have been established and consolidated, a very advanced legislation framework has been put in place and there has been a constructive approach to regional co–operation. The government of Kosovo has worked with its full competence and commitment to building strong, accountable and transparent democratic institutions, a pro- fessional internationally trained police force, and above all, to promote international hu- man rights standards and community rights that are granted by the Constitution of Kosovo." (Maddock, 2013)

Conclusions and Recommendations

The only way for Small Countries to deal with cyber security problems successfully is to reduce unmanageable complexities to a manageable level through the implementation of various developments and smart policies. That can be achieved through the application of strategic thinking, a comprehensive approach, an appropriate system concept and brave de- cisions. Our current analysis were based on our earlier published research results and on information related to the latest challenges and developments. As a result, we have reached the following conclusions:

1. International or global tendencies aiming to strengthen cyber security and the elimina- tion of backfire security solutions should be researched and supported. The opportunities inherent in these processes should be exploited. This will significantly reduce the scope of problems to be solved with the use of own resources;

19 This proposal was first made in 1999, when we thought that certain countries were unable to fight against the insatiable appetite of their security institutions for information. (Nagy, 1999: 182)

20 Today, at the time of the Snowden scandal (Lee, 2013), little is said about the efforts made in the US to resolve the conflict between privacy rights and the collection of information to counter terrorist activities. It is enough to mention the National Strategy for Trusted Identities in Cyberspace (The White House, 2001), or the NIST Grants (PBA, 2012), which well illustrates these efforts.

2. Efforts directed at the use of backfire policies by internal or external interest groups should be resisted. In order to recognize such policies and counter the various types of pressure applied, scientific means available for the acquisition of information, analytical methods and wide ranging international collaboration should be applied. That will pro- tect the governments of Small Countries from unnecessary losses, dangerous solutions and serious security risks. One should be able to say " no", which is not always easy for small and therefore exposed countries;
3. ICT and cyber security developments should be integrated into a unified system. The purchase of services and the exploitation of the opportunities offered by cloud computing should be preferred to investments. The availability of service based ICT infrastructure should be supported by appropriate regulation, standardization, control, and good con- tracts. This will both reduce ICT and security costs and place the burden of the security problems of Small Countries on the shoulders of large multinational service providers with a much wider range of resources;
4. The solution of cyber security problems should be supported through the establishment of specialized knowledge centres and security culture programs;
5. Regardless of internal political conditions, international collaboration in the field of cy- ber security should be integrated into the collaboration system of NATO Cyber Defence.

In order to successfully deal with their cyber security problems, Small Countries should apply the following schemes:

- Minimize the scope of problems to be solved with own resources through appropriate ICT developments, outsourcing, purchase of services, and the development and use of secure systems;
- Spread the remaining problems among authentic domestic and international security col- laboration systems;
- Avoid wrong directions, fake solutions, anachronistic developments and backfire solu- tions and recognize risks that cannot be covered through sensible expenditure, aiming at appropriate contingency planning.

The realization of the above depends mainly on professional competence and the persua- sion of supporting foreign powers and domestic political forces instead of the use of financial resources. In this work, the most important supporter of Small Countries is the public. The support of the public can be gained through the use of privacy policies, which are

in accor- dance with the Universal Declaration of Human Rights. If Small Countries enter the mire of secrecy for security reasons, they can only loose.

References

BASULTO, D. (2010): Digital deterrents: Preventing a Pearl Harbor of cyberspace. *The Washington Post*, 20 12 2010, http://www.washingtonpost.com/blogs/innovations/post/digital- deterrents-preventing-a-pearl-harbor-of-cyberspace/2010/12/20/gIQASNKyoL_blog.html (downloaded: 13 06 2013)

CABINET OFFICE (2011): *UK Cyber Security Strategy, Protecting and promoting the UK in a digital world.* London, https://www.gov.uk/government/uploads/system/uploads/attachment_ data/file/60961/uk-cyber-security-strategy-final.pdf (downloaded: 21 07 2013)

CASTELLS, M. (1996): *The Information Age – Economy, Society and Culture.* Oxford: Blackwell Publishers

CHAUM, D. (1992): Achieving Electronic Privacy. *Scientific American*, pp. 96–101.

CORNELL UNIVERSITY LAW SCHOOL (2002): *Cyber Security Enhancement Act of 2002* (6 USC § 145). http://www.law.cornell.edu/uscode/text/6/145 (downloaded: 29 06 2013)

DAVIS, J. (2011): NATO after 9/11: a US perspective. *NATO Review*, http://www.nato.int/docu/review/2011/11-september/NATO-US-Perspective-9-11/EN/index.htm (downloaded: 13 06 2013)

GALLAGHER, S. (2013): *US, Russia to install "cyber-hotline" to prevent accidental cyber war*. http://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to- prevent-accidental-cyberwar/ (downloaded: 13 06 2013)

GENERAL DYNAMICS INFORMATION TECHNOLOGY (2011): *General Dynamics Awarded $122 Million IT Support Task Order by the U.S. Army, Europe.* http://usacybersecurityjobs. com/2011/01/05/general-dynamics-awarded-122-million-it-support-task-order-by-the-u-s- army-europe/ (downloaded: 01 06 2013)

ITSKOV, D. (2012): *The path to neo–humanity as the foundation of the ideology of the "Evolution 2045".* http://www.2045.com/articles/30869.htm (downloaded: 13 06 2013) KOSOVO's NEW DIPLOMAT (2013): Kosovo Digital Diplomacy Strategy reviewed as one of the best in Europe. *Kosovo's New Diplomat* (Bi-monthly newsletter of Ministry of Foreign Affairs of Republic of Kosovo), Double Issue. No. 8–9, Year III., http://www.mfa-ks.net/ repository/docs/20130403-0809-newspaper-KND-WEB.pdf (downloaded: 13 06 2013)

KOVÁCS L. (2009): Electronic Warfare And The Asymmetric Challenges. *Bolyai Szemle*, Vol. 3, pp. 135–151. ISSN 1416-1443

KOVÁCS L., KRASZNAY Cs. (2010): Digitális Mohács (Egy kibertámadás forgatókönyve Magyarország ellen. *Nemzet és Biztonság*, February, pp. 44–57. ISSN 1789–5286

LEE, M. V. (2013): State Department revokes NSA leaker Snowden's passport. *The Associated Press*, June 23, http://www.news1130.com/2013/06/23/ap-source-state-department-revokes- nsa-leaker-snowdens-passport/ (downloaded: 23 06 2013)

LEE, R. M. (2012): *Stuxnet and Cyber Deterrence. Infosecisland*. http://www.infosecisland.com/blogview/22168-Stuxnet-and-Cyber-Deterrence.html (downloaded: 01 06 2013)

LETTER FROM THE CAPITOL (2010): Cyberwar Guru Warns Again of Digital Pearl Harbor. *Letter from the Capitol*, April 16, http://www.letterfromthecapitol.com/ letterfromthecapitol/2010/04/cyberwar-a-guru-warns-again-of-digital-pearl-harbor.html (downloaded: 13 06 2013)

LIBICKI, M. C. (2012): Cyberspace is not a Warfighting Domain. *A Journal of Law and Policy for the Information Society*, Vol. 8, Issue 2, pp. 322–336. http://moritzlaw.osu.edu/students/ groups/is/files/2012/02/4.Libicki.pdf (downloaded: 13 06 2013)

MADDOCK, C. (2013): *Kosovo, the youngest nation in Europe. A success story of democratic and multi–ethnic state building: Ambassador Shkendije Geci Sherifi.* Interview, Budapest, 22 February, http://www.budapesttimes.hu/2013/02/22/kosovo-the-youngest-nation-in-europe/ (downloaded: 13 03 2013)

NAGY K. (1996): Security of virtual worlds. *Tudományos és Műszaki Tájékoztatás*, Vol. 4-5, pp. 148–154. ISSN 0041–3917

NAGY K. (1999): Secret and Security in Information Society. *Belügyi Szemle*, Vol. 4-5, pp. 172–183. ISSN 1218–8956

NAGY K. (2001): *The role of knowledge centres in the evolution of the global informational society*. In. Management of Engineering and Technology, 2001. PICMET '01, Portland International Conference on, Vol. 1. ISBN 1–890843–06–7, http://dx.doi.org/10.1109/ PICMET.2001.951806 (downloaded: 21 07 2013)

NAGY K. (2007a): Slowing down of Globalisation and the European Security. *Szakmai Szemle*, Special Issue, pp. 44–54. ISSN 1785–1181

NAGY K. (2007b): *The Role of Knowledge Centres in the Information Warfare.* In. Lecture at the 6th European Conference on Information Warfare and Security, Shrivenham: Defence

College of Management and Technology, July 2–3, Published in the conference publication, pp. 181–186. ISBN 978-1-905305-49-0 Cd

NAGY K. (2007c): The role of knowledge centres in the development of new security culture. *Szakmai Szemle*, Vol. 1, pp. 172–184. ISSN 1785–1181

NAGY K. (2008): *The Specialties of the New Security Culture Program. Presentation at the 'Security Culture of the 21st Century'.* Conference at Zrínyi Miklós University of National Defence on June 13. Published in Gondolatok és Vélemények a biztonságunkról, pp. 29–38. ISBN 978–963–06–6370–0
NAGY K. (2009a): The additional benefits of setting up an energy security centre. *Energy* Vol. 34, Issue 10, pp. 1715–20. http://dx.doi.org/10.1016/j.energy. 2009. 07. 038. (downloaded: 13 06 2013)
NAGY K. (2009b): *The IT Infrastructure of Virtual Knowledge Centres.* In. Lecture at the eChallenges e-2009 International Conference, October 21–23. Istanbul, ISBN 978–1–905824–13–7
NAGY K., KARASSZON A. (2008): Aid Economies – Slack of Globalization. *Hadtudomány*, pp. 34–36. ISSN 1215–4121
NAGY K., KÖRMENDI K. (2012): Use of renewable energy sources in light of the "New Energy Strategy for Europe 2011–2020". *Applied Energy*, Volume 96, pp. 393–399. http://dx.doi.org/10.1016/j.apenergy.2012.02.066 (downloaded: 16 06 2013)
NATO (2011): *New threats: the cyber-dimension. NATO Review.* http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm (downloaded: 04 07 2013) NATO (2012a): *Secretary General's Annual Report.* http://www.nato.int/cps/en/natolive/opinions_94220.htm?selectedLocale=en (downloaded: 01 06 2013)
NATO (2013a): *North Atlantic Council visits KFOR 03.* http://www.nato.int/cps/en/SID-54EDA853-B3867636/natolive/news_102109.htm (downloaded: 04 07 2013)
NATO (2013b): *NATO and Cyber Defence.* http://www.nato.int/cps/en/SID-565C1CD5-36861BC5/natolive/topics_78170.htm? (downloaded: 13 06 2013)
NATO (2013c): *NATO and Colombia open channel for future cooperation.* http://www.nato.int/cps/en/SID-888A4741-12135303/natolive/news_101634.htm (downloaded: 26 06 2013)
NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). https://www.ccdcoe.org/www.ccdcoe.org/ (downloaded: 19 06 2013)
NOJEIM, G. T. (2012): Cybersecurity: Ideas Whose Time Has Not Come–and Shouldn't. *A Journal of Law and Policy for the Information Society*, Vol. 8, Issue 2, pp. 408–432. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Nojeim.pdf (downloaded: 13 06 2013)
OECD (2002): *OECD Guidelines for the Security of Information Systems and Networks*, 1037th Session of the OECD Council, 25 July, http://www.oecd.org/sti/ieconomy/31670189.pdf (downloaded: 13 06 2013)
PARRISH, K. (2012): *Kaspersky: International Cyber Weapons Agreement Needed.* In. iTWire, May 23, http://www-01.ibm.com/software/solutions/smartwork/healthcare.jsp (downloaded: 13 06 2013)
PETERMAN, L. (1993): Privacy's Background. *Cambridge University Journal* Column: The Review of Politics, Vol. 55 Issue 02, pp 217–246. DOI: http://dx.doi.org/10.1017/ S0034670500017368 (About DOI), (Published online: 05 August 2009)
PUBLIC AND BUSINESS AFFAIRS (PBA) (2012): *NIST Seeks Proposals for Projects to Improve Trust in Cyberspace.* From NIST Tech Beat: February 7, http://www.nist.gov/public_ affairs/releases/nstic-comp-020712.cfm (downloaded: 13 06 2013)
SZABÓ K. (1985): *Proportionality principle and value in the modern economy.* Budapest: Akademia Kiadó, ISBN 963 05 3300 6 (in Hungarian)
THE WHITE HOUSE (2001): *National Strategy for Trusted Identities in Cyberspace.* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (downloaded: 17 06 2013)

THE WHITE HOUSE (2013): *Executive Order — Improving Critical Infrastructure Cybersecurity.* Office of the Press Secretary, February 12, http://www.whitehouse.gov/the- press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (downloaded: 13 07 2013)
UN GENERAL ASSEMBLY (2004): *Creation of a global culture of cybersecurity and the protection of critical information infrastructures 58/199*. Resolution adopted by the General Assembly, 30 January, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_ resolution_58_199.pdf (downloaded: 13 06 2013)
VÁRHEGYI I., MAKKAY I. (2000): *Information Age, Information Warfare, Security Culture.* Budapest: OMIKK, ISBN 963 593 238–3