AARMS Vol. 18, No. 2 (2019) 65–76.

DOI: 10.32565/aarms.2019.2.9

National Cybersecurity Strategy Framework[1]

László KOVÁCS[2]

Cyberspace and its services and the digital-based processes affect all segments of our lives. These effects are felt in the economy, politics, culture, but also in individual elements of our private life and in people's relationships, as well. Accordingly, one of the biggest challenges for cyber security is that we highly depend on these services. Most of the countries have realised that today cyber security is one of the essential parts of their national security. Its reason is twofold. Firstly, the digital ecosystem is vital for a nation and this ecosystem cannot work properly without cyber security, secondly there is no alternatives to avoid the aforementioned dependence. As a result, cyberspace and its security are of decisive importance to countries with advanced information infrastructures. However, national cyber security strategies, whether they are made by big powers or small countries, have different answers to the challenges of cyberspace. At first, this paper focuses on these challenges and then tries to identify some unified elements which could be the main pillars of an effective national cyber security strategy.

Keywords: *cyber security, strategy, national security*

Introduction

One of the most important strategic documents of developed countries is the national security strategy. In its national security strategy, the country presents its ideas of achieving the protection of all values and interests that have been defined in the constitution of the state.

The strategy builds on this encompassing the security environment that defines values and interests, outlining the challenges and threats of today and the near future.

Further on, the strategy encompasses the security environment that also determines these values and interests, as well as the present and future challenges and threats to them.

Based on the analysis and assessment of these threats and challenges, the strategy gives the most important goals that could provide an adequate response to the challenges and threats identified. The strategy assigns tasks and activities to these goals and determines the necessary organisational, legislative and financial resources.

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-15-2016-00001 entitled "Public Service Development Establishing Good Governance" in the Lőrincz Lajos Professor Program. This paper highly based on the author's main conclusions expressed in his doctoral thesis of the Hungarian Academy of Sciences.

[2] Ph.D., Brigadier General, Professor, National University of Public Service, Faculty of Military Science and Officer Training, Department of Electronic Warfare; e-mail: kovacs.laszlo@uni-nke.hu; ORCID: 0000-0002-6403-0650

The national security strategy of the country is supported by sectoral strategies. Sectoral strategies reflect specific elements of security in the given sector. Accordingly, the national cyber security strategy, as one of the sectoral strategies, reflects the interests of the country and the strategic objectives for the protection of these interests in the cyberspace. The national cyber security strategy should return to address the threats and challenges identified in the national security strategy and, in parallel, support the strategic objectives set out in the national security strategy by addressing the challenges posed by cyberspace.

At first, this paper will present and briefly analyse the challenges and threats relevant to the strategic environment of cyber security. The main objective is to focus on trends that are related to the development of a cyber security strategy that fundamentally affect the content of a national cyber security strategy.

Strategic Threats to National Cyber Security

Most of the national security strategies of the European countries list and analyse the most severe strategic threats to the country and its interests. These are usually the following: cybercrime; cyber espionage; hacktivism; hybrid warfare and serious cyberattacks; proliferation of cyber weapons; serious attacks against critical infrastructures and critical information infrastructures.

Before we analyse the strategic answers to these strategic threats and challenges, it is needed to briefly examine some of these threats.

Table 1. *Strategic threats in the national cyber security strategy of Austria, the Czech Republic, Hungary and the United Kingdom.*
(Edited by author based on: Austria [11], the Czech Republic [13], Hungary [16], the United Kingdom [3].)

Country	**Strategic threats, risks and challenges**
Austria	Risks: • cybercrime • identity fraud • cyberattacks • misuse of the Internet for extremist purposes

Country	Strategic threats, risks and challenges
The Czech Republic	Challenges: • the Czech Republic as a potential test bed • lack of the public's trust in the state • increased number of Internet and ICT users and increased criticality of technology failures • increasing amount of mobile malware along with the increased number of mobile device users • possible information exfiltration through a hardware backdoor • Internet of Things • security risks related to the transition of IPv4 to IPv6 • security risks related to the electrification of public administration (eGovernment) • insufficient security of small and medium enterprises • big data, new data storage environments • protection of industrial control systems and of information systems in the health sector • smart grids • increased ICT dependence of the state's defence forces • increasingly sophisticated malware • botnets and DDoS/DoS attacks • increase in cybercrime • threats and risks related to the use of online social networks • low digital literacy of end users • shortage of cyber security experts and the need for curricula reform
Hungary	Threats: • information warfare against ICT systems of critical infrastructures • lack of properly regulated information security in ICT systems • emerging new technologies: i.e. cloud, mobile internet
The United Kingdom	Threats: • cybercriminals • states and state-sponsored threats • terrorists • hacktivists • script kiddies Vulnerabilities: • an expanding range of devices • poor cyber hygiene and compliance • insufficient training and skills • legacy and unpatched systems • availability of hacking resources

The cybercrime methods nowadays are more and more built on each other, and the cybercrime complexity is increasingly being observed. Users are targeted by identity theft and phishing attacks, as well. At the same time, these methods are combined and they are more complicated than before. Accordingly, it is more difficult to detect them and more sophisticated technical and procedural activities are needed to discover them. These attacks aim at not just the users but in many cases the real target is the users' company that could be an industrial company or even a financial institution. The offender, that is the cybercriminal, is no longer a lone perpetrator, because complex security solutions require a complex attack modus operandi. Additionally, it must be based on complex knowledge and thus multiple elements to commit a single offense. Thus, increasingly organised groups

are the perpetrators. Cybercrime, in many cases, requires serious financial investment due to these advanced and increasingly complex defence systems. Thus, often the traditional criminal circles are those who make such investments. They buy or rent the knowledge and technical background that is necessary for the realisation of the crimes. [1]

At the same time, cybercrime and those who are involved in it, for long years not only gain high technical knowledge but also receive information that can be of interest to the strategic level, as well. The data gathered from cybercrime and the conclusions drawn from their analysis can be used to influence political or economic processes in another country. [1]

Initially, cyber espionage was like industrial and economic espionage, as one of the most important goals of obtaining information that is used by or through computers and Info Communication Technology (ICT) tools was the theft of intellectual products. Today, however, we are witnessing more and more marked changes in this area. Cyber espionage is still present alongside the acquisition of economic information, but the targets of cyber espionage include public administration, governmental and nongovernmental organisations of the defence sphere. One form of cyber espionage is the Advanced Persistent Threat (APT) attack. APT is a combination of various cyberattacks. This is a complex process involving several very sophisticated malwares and attacking procedures, which are very hard to detect or discover. One of the most important attributes of APT attacks is that they are largely undiscovered for a long time and remain unnoticed. Attacks are typically characterised by the fact that they do not target accidental targets, but rather their targets are pre-selected networks and systems that handle valuable political, business, military, or administrative information valuable to the attacker. APT attacks that are well-prepared typically last for a long time from one to two weeks or up to years. APT attacks are executed by non-random targeting software robots, but by programs designed to deliberately focus targets that detect weak or vulnerable points by sophisticated procedures and then penetrate the system, the real purpose of which is to unconsciously capture the data stored there and attack the attacker. [1]

At the beginning of the 2000s, hacktivism was defined as "[…] the group of hackers and artists who coined the phrase, was intended to refer to the development and use of technology to foster human rights and the open exchange of information". [2] Today, thanks to the Anonymous group, hacktivism itself is unchanged. However, its methods and mainly its targets are much more dangerous for the governments. Therefore, many countries' national cyber security strategies deal with it as a source of threat. The UK's national cyber security strategy formulates the hacktivism and hacktivists as follow: "Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to inflict greater and lasting damage on their victims." [3]

The importance of critical infrastructures and critical information infrastructures in our everyday life is unquestionable. Since these systems are the most important components of our digital era, and without them our everyday life is hardly imaginable, we must take into consideration their vulnerability by assessing the consequences of possible attacks. Critical infrastructures, as well as critical information infrastructures are exposed to physical hazards, so handling and preparing for them is vital. As info communication systems are also built in physical space, their total or partial physical damage will lead to system shutdowns and shorter service life. This is therefore the primary source of danger. At the same time,

these infrastructures are threatened not only by physical but also by cyber threats. This is the second most important source of threats because the features of cyberspace, such as limitlessness, openness, globality, software and hardware vulnerabilities, can be attacked by global, regional, national or even lower levels. As evidenced by the case of the Stuxnet worm virus applied to Iranian nuclear facilities, the attack of critical infrastructures is indirectly possible, including cyberattacks primarily related to critical information infrastructures, which can cause the greatest extent damage. When exploring the causes of the most serious vulnerabilities in critical infrastructures, we must conclude that these systems and components are extremely heterogeneous. This is the most commonly encountered in the parallel operation of the former and the latest technology constituents. One of the best examples is Supervisory Control and Data Acquisition (SCADA) systems. The concomitant application and daily use of old and new assets in critical infrastructures is most visible in the energy sector, as "the use of new technology in cost-effective energy production, storage and transport is increasingly at the beginning of important considerations and priorities". [1] IoT (Internet of Things) tools that appear in critical infrastructures, mainly in their control, increase the vulnerability of the systems from the point of view of the danger, since it is even more true that not only the earlier but the newest technology is present in the infrastructures simultaneously. The older technology is vulnerable through its software and hardware components; meanwhile, the new technology can be attacked through its remote connections, as well. [1]

Strategy and Its Elements to Handle the Threats on National Cyber Security

Today, the majority of countries have national cyber security strategies. These strategies are mostly static documents that do not or only partially handle the dynamism that characterises cyberspace. However, due to the nature of cyberspace, i.e. globality, border lessness, and extremely rapid technological changes, as the main characteristics, require that we define a unified model or even its elements for creating a national cyber security strategy which can really be of use. Therefore, we should identify elements of current national cyber security strategies of different countries that are either similar or identical and which can be the basis for a national cyber security strategy model. In this work, we have to take into consideration the relevant requirements and regulations of international organisations, i.e. the European Union or NATO.

Conclusions from the cyber security strategy and relevant policies of the European Union, NATO and four EU countries

Previously, I have analysed several national cyber security strategies of European countries and parallel with this work, the EU's and NATO's main policies and strategies in cyber security and cyber defence have also been analysed. [1][4] Based on those works, hereby I summarise the main elements of the different international organisations' (EU and NATO) and four of the analysed countries' cyber strategies.

My conclusions from the Cyber Security Strategy and relevant policies of the European Union are as follows:

- the EU Cyber Security Strategy[3] aims to enhance the resilience of Member States and the EU towards cyberattacks;
- the strategy defines the common security and defence policy framework for cyber defence;
- the NIS Directive[4] sets out the task of Member States to prepare the national cyber security strategy;
- based on NIS, the national cyber security strategy should also include critical infrastructure protection tasks;
- some elements of the national organisational system for cyber security, including for EU liaison, are also defined by NIS. [5]

Conclusions from the cyber security policies and regulations of NATO:

- the interpretation of cyberspace as a domain of warfare[5] has many consequences for member states (for example, delegating broader cyber defence tasks to the army, building cyberattack capabilities, setting up cyber commands);
- one of the NATO Cyber Pledge[6] is to approximate the currently different levels of cyber defence capabilities of member states;
- NATO's Cyber Operation Centre can play an important role not only in military but also in the civil defence;
- the Alliance promotes the strengthening of international cooperation between both member states and non-NATO countries. [5]

Conclusions from Austria's national security[7] and national cyber security strategy:[8]

- cyber security plays an important role in the national security strategy of Austria;
- the curbing of cybercrime and the necessary organisational background of cyber security are important goals in the national security strategy;
- the national security strategy also defines military cyber capabilities;
- the national security strategy requires the preparation of a national cyber security strategy;

---

3 Its official title is *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. [6]

4 NIS Directive: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6th July 2016 concerning measures for a high common level of security of network and information systems across the Union. The main aim of NIS "[…] lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market". [7]

5 NATO has recognised cyberspace as a domain of warfare at the Warsaw Summit in 2016. The official communiqué of the Warsaw Summit formulated it as follows: "Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success." [8]

6 NATO, at the Warsaw Summit, as well, declared a plan to ensure and foster the Alliance's common efforts on cyber defence that is called pledge. According to the official text, the Allied Heads of State and Government of Member States of NATO: "pledge to ensure the Alliance keeps pace with the fast-evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea." [9]

7 Austrian Security Strategy Security in a New Decade—Shaping Security. [10]

8 Austrian Cyber Security Strategy. [11]

- the national cyber security strategy also addresses the technical hazards;
- a special cyber risk matrix has been built into the cyber security strategy;
- cyber security strategy defines the most important elements of organisational background;
- it encourages R&D activities and international cooperation in cyber security;
- one of the strategic goals of Austria is to increase PPP in cyber security. [5]

Conclusions from the Czech Republic's strategies:[9]

- the country issued a forward-looking national security strategy in 2015 which contains provisions for the protection of critical infrastructures and military information systems, defines the preparation of the national cyber security strategy and describes the organisational system of cyber security in detail;
- the second edition of the national cyber security strategy is alive, along with an action plan[10] which defines the organisational background of cyber security;
- this strategy assigns tasks to critical infrastructure protection as well as enhancing cooperation between the private and public sectors;
- it encourages the R&D and increases the anti-cybercrime activity with the establishment of an effective legal environment;
- the strategy also emphasises the importance of international cooperation. [5]

Conclusions from Hungary's strategies:[11]

- Hungary's national security strategy contains important references to cyber security and the importance of cyberspace. The strategy is currently under review, inter alia, because of the changed security situation and the emerging security challenges;
- the national military strategy also counts on the dangers of cyberspace, determines the enhancement of cyber defence of the Hungarian Defence Forces and refers to the cyber warfare. At the same time, there has been no progress in the field of cyber warfare either at strategic or organisational level in Hungary. This strategy is also under review;
- the national cyber security strategy was completed more than five years ago;
- the national cyber security strategy is very sketchy, but it also has a suitable system of tasks, and also has a strategic organisational background in order to create or increase cyber security;
- the strategy provided an adequate basis for the development of cyber regulation (for example, the adoption of the Electronic Information Law)[12] and the launching of social consultations and co-operations;
- this strategy is currently under a reviewing process. [5]

---

9 National Security Strategy of the Czech Republic, [12] and the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. [13]

10 Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020. [14]

11 Hungary's National Security Strategy, [15] National Cyber Security Strategy of Hungary, [16] Hungary's National Military Strategy. [17]

12 Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies. [18]

Conclusions from the United Kingdom's strategies:[13]

- the UK's national security strategy considers cyberspace to be of strategic importance, within which it has undergone several updates, but each one counts on the importance of information technology and indicates the United Kingdom as a cyber power;
- the national security strategy counts on cyber threats, which also address strategic goals;
- the national security strategy assigns tasks to the Army for cyberspace;
- one of the main philosophical elements of the national defence strategy is deterrence, which also focuses on cyberattacks;
- the importance of critical infrastructure protection has been included in the strategic goals;
- the second edition of the national cyber security strategy is currently in force;
- it defines responsibilities for a wide range of actors in society to create cyber security;
- the strategy assigns organisational background to the coordination of tasks;
- it also includes an implementation plan for implementing different tasks;
- the strategy also defines the formation of cyberattack capacities;
- the development of cyber security integrates cyber security awareness, development of an industry support background, and continuous monitoring of technological and policy changes and their inclusion in cyber security;
- the importance of international cooperation is highlighted. [5]

Possible Elements of a National Cyber Security Strategy

On the basis of my suggestion, the National Cyber Security Strategy should include the following elements:

- a collection of terminology which defines both cyberspace and cyber security;
- evaluation of the strategic environment: presenting the cyber threats, challenges, risks and vulnerabilities;
- identifying the strategic goals that contribute to achieving strategic national security goals by creating and continuously increasing cyber security;
- strategic ideas for implementing the organisational background of cyber security;
- definitions of critical information infrastructures and critical infrastructure protection;
- strategic support for R&D innovation in the field of cyber security;
- a cyber security education strategy that aims to develop and enhance cyber security awareness;
- strategic stimulation of mutual co-operation between public and private cyber security (PPP);
- declaring commitment to international cyber security cooperation;
- the action plan for achieving strategic goals;
- developing an evaluation system that gives indicators in the strategy and on the control of the implementation of the action plan. [5]

[13] National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom. [19] National Cyber Security Strategy 2016–2021. [3]

In addition to this, it is important to emphasise that, depending on the country's political decision, the role of the military should be expedient in the country's defence. This may address the following issues (areas and related purposes):

- creating the military's cyber capabilities, including cyberattack capabilities;
- the tasks of the armed forces in protecting the country and possibly protecting critical infrastructures and critical information infrastructures;
- the tasks of the armed forces in a responsive cyberattack. [5]

These cyber capabilities of the armed forces with sufficiently robust state-of-the-art cyber defence organisations and their cyber defence capabilities could be deterrent. [5]

The Model of a National Cyber Security Strategy

Based on the conclusions drawn from the analysed national cyber security strategies, and also taking into account the summarised experiences of the modelling examples so far, the following general proposal has been made for building up the national cyber security strategy with the aforementioned important content elements.

The model has four phases, each corresponding to the requirements of the given phase with continuously changing activities. The proposed model can apply for 3–4 years, but sometimes longer cycles are possible. Dynamic variables at different phases of the model, such as measurement results or the assessment and adaptation of hazards and challenges, can be carried out in a 3–4-year cycle without having to change it basically, for example, by generically transforming the basic cyber security organisational background. Obviously, the current and medium-term changes in cyberspace, as well as the technical and human changes, such as the artificially intelligent technical uses and its indirect impact on the human environment will necessitate a revision of the bases of the strategy every 4–5 years. [5]

The four phases of the suggested model are the following:[14]

- Phase 1: Creating a new strategy/modifying an old strategy:
  - define the general purpose of the strategy, if necessary revise it;
  - revising of existing cyber policies and cyber related regulations;
  - plan for critical infrastructure and critical information infrastructure protection;
  - revising of information sharing policies.
- Phase 2: Introduction and implementation of the new strategy (amendment of an earlier strategy if necessary):
  - set up an effective organisational and management structure;
  - developing and clarifying cyber security emergency plans;
  - developing incident management capabilities;
  - enhance effective actions against cybercrime both domestically and internationally;
  - establish public–private partnerships;
  - increasing the efficiency of cooperation between the public sector institutions.

[14] According to the suggested model every phase followed by a feedback session where the effectiveness of certain phase is checked and if necessary the required minor adjustments could be done.

- Phase 3: Operation of a cyber security system based on the new (modified) strategy:
  - organising cyber security exercises;
  - development and encouragement of cyber-training and education programs;
  - increasing the citizens' cyber security awareness.
- Phase 4: Evaluation of the strategy and its effectiveness:
  - continuous development of the strategy;
  - adjustment of the national cyber security strategy using the results of key performance indicators;
  - processing the experiences gained during the cyber exercises and, on the basis of these, elaborating efficiency-enhancing measures. [5]

It is important to emphasise that the proposed model is not designed to produce a static document, but it can dynamically manage the most diverse challenges and threats that emerge in cyberspace, and capable of delivering cyber security for the given country.

Conclusions

Today, cyberspace and its security for countries with advanced information infrastructure are critical. This fact must be reflected in the national strategic vision of cyber security.

Analysing the context of the national security strategies and the national cyber security strategies of different countries, it can be found that cyber security is one of the most important factors to achieve the most important objectives of the national security strategy.

When we consider the strategic challenges in cyberspace, we find that there have been a number of threats such as cybercrime, hacktivism, or cyber espionage. However, a new, very serious challenge has emerged over the last half decade that can be summarised in state-aided cyberattacks. These cyberattacks use various attacking methods in systematic and very sophisticated ways. All of these cyber threats and challenges require strategic cyber defence solutions both at international and national level.

When we analyse cyber security strategies in some European countries, we can observe that although these countries follow different approaches to create valuable and robust cyber security, still many elements can be identified in these different ways that are highly resembling each other.

In this paper, these nearly same elements have been identified, and depending on their role and their effectiveness, they can be the basis for a national cyber security strategy model. Based on this, using my previous findings in relation to common elements and the effective and truly active elements revealed in the cyber security activities of the countries under investigation, I proposed a model with the key elements to create a national cyber security strategy.

References

[1] KOVÁCS L.: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus Kiadó, 2012.

[2] Wired Staff: Hacktivism and How It Got Here. *Wired*, 07.14.2004. www.wired.com/2004/07/hacktivism-and-how-it-got-here/ (Downloaded: 11.11.2018)
[3] *UK's National Cyber Security Strategy 2016–2021.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Downloaded: 11.11.2018)
[4] KOVÁCS L.: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. *Hadmérnök*, 7 2 (2012), 302–311.
[5] KOVÁCS L.: *Strategic Approach of Cyber Security.* Doctoral Thesis of the Hungarian Academy of Sciences (Draft). Budapest, MTA, 2018.
[6] *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Downloaded: 11.11.2018)
[7] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN (Downloaded: 11.11.2018)
[8] *NATO Warsaw Summit Communiqué.* www.nato.int/cps/en/natohq/official_texts_133169.htm (Downloaded: 11.11.2018)
[9] *NATO Cyber Defence Pledge.* www.nato.int/cps/su/natohq/official_texts_133177.htm (Downloaded: 11.11.2018)
[10] *Austrian Security Strategy: Security in a New Decade – Shaping Security.* www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf (Downloaded: 11.11.2018)
[11] *Austrian Cyber Security Strategy.* www.digitales.oesterreich.gv.at/documents/22124/30428/AustrianCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21 (Downloaded: 11.11.2018)
[12] *Security Strategy of the Czech Republic 2015.* www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf (Downloaded: 11.11.2018)
[13] *National Cyber Security Strategy of the Czech Republic from the Period of 2015 to 2020.* www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (Downloaded: 11.11.2018)
[14] *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf (Downloaded: 11.11.2018)
[15] *1035/2012 (21 March) Government Decree on the Hungary's National Security Strategy.* www.ecfr.eu/page/-/Hongrie_-_2012_-_National_Security_Strategy.pdf (Downloaded: 11.11.2018)
[16] *1139/2013 (21 March) Government Decision on the National Cyber Security Strategy of Hungary.* www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx (Downloaded: 11.11.2018)
[17] *1656/2012 (20 December) Government Decree on Hungary's National Military Strategy.* http://2010-2014.kormany.hu/download/b/ae/e0000/national_military_strategy.pdf#!DocumentBrowse (Downloaded: 11.11.2018)
[18] *Hungarian Act L of 2013 on Electronic Security of State and Local Government Bodies.*

[19] *National Secrity Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (Downloaded: 11.11.2018)