CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

László Kovács

Gergely Szentgáli

National Cyber Security Organisation: HUNGARY

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Upcoming in 2015

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of October 2015.

About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations and Austria as a Contributing Participant. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

HUNGARY

By László Kovács
University Professor, National University of Public Service, Hungary

and

Gergely Szentgáli
Defence Policy Officer, Ministry of Defence, Hungary

Table of Contents

1. Introduction: information society in Hungary

Hungary issued the nation's first *National Information Strategy*[1] in 2001, which was followed by the renewed *Hungarian Information Society Strategy*[2] in 2003. After the first strategies, each government has made steps towards an information and knowledge based society and economy. In 2010, a *Digital Renewal Action Plan*[3] was issued, which included four main pillars (action plans) and more than 80 action proposals. This plan was based on main strategic goals and recommendations of *Digital Agenda for Europe 2020*.

The *National Info-communication Strategy* (NIS)[4] sets out the basis for info-communication developments to be implemented by 2020. The strategy, issued in early 2014, outlined the primary objectives of the 2014-2020 period focusing on the fields of digital infrastructure, competence, economy and state.[5] In accordance with the main goals of NIS, every household should have internet access of at least 30 Mbps and at least half of them of 100 Mbps or faster by 2018. The NIS includes a plan for the full National Telecommunication Backbone Network to be established by 2016. Further goals include mobile broadband coverage which should reach 95% by 2016, by which date broadband internet access of at least 20 Mbps should be accessible for all educational institutions.[6]

1.1. Internet infrastructure availability and take-up

Hungarian households with access to the internet at home numbered more than 7.5 million at the beginning of 2015. This is 75% penetration rate referring to the 10 million population of Hungary and ranks the country 17th among the EU28.[7] In 2011, this rate was only 65% which was 18th among EU countries.[8]

The number of mobile phone subscriptions reached 11.8 million in the 1st quarter of 2015. Mobile internet subscriptions comprise 65% of total internet access.[9]

Wired internet access is based on two main technologies: cable network, which makes up 17% of total internet access and which grew 6.5% in 2014, and xDSL subscription (11% of total internet access) which grew by 1.4%.[10]

Standard fixed broadband is available in 94% of households, which ranks 23rd in the EU.[11] With regard to broadband quality available to subscribers, 83% of subscribers are offered speeds exceeding 10 Mbps and 40%

[1] National Information Society Strategy, Budapest 2001. Cited in 'Report on Hungarian Information Society 1998-2008'. <http://infoter.eu/attachment/0003/2817_ittk_mitj_1998_2008.pdf>.
[2] ibid.
[3] Digital Renewal Action Plan. <http://infoter.eu/alapdokumentumok/digitalis_megujulas_cselekvesi_terv>.
[4] National Info-communication Strategy. <http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf>.
[5] ibid.
[6] Ministry of National Development: National Info-communication Strategy: Fully electronic services in public administration within four years. <http://2010-2014.kormany.hu/en/ministry-of-national-development/news/national-info-communication-strategy-fully-electronic-services-in-public-administration-within-four-years>.
[7] EU Digital Agenda, 'Country Ranking Table, On A Thematic Group of Indicators — Digital Agenda Scoreboard', 2014. < http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"internet-usage","ref-area":"HU","time-period":"2014"}>.
[8] ibid.
[9] Hungarian Central Statistical Office: Statistic Mirror. 43/2015. <http://www.ksh.hu/docs/hun/xftp/gyor/tav/tav1503.pdf>.
[10] ibid.
[11] EU Digital Agenda, 'Country Ranking Table, On A Thematic Group of Indicators — Digital Agenda Scoreboard', 2014. <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"broadband","ref-area":"HU","time-period":"2014"}>.

speeds over 30 Mbps, both of which are significantly higher than the EU average of 72% and 26%, respectively.[12]

1.2. Availability and use of e-services

1.2.1. E-government

Hungary has established various e-Government services and different electronic administration tools during the last decade. The amendment of *Act CXL of 2004 on the General Rules of Administrative Procedures and Services by Act CLXXIV of 2011* set a legal base for these services in April 2012.[13]

The institutional framework for e-Government has also been founded, based on state-owned agencies and institutions. The **Central Office for Administrative and Electronic Public Services**, an agency of the Ministry of Interior, operates the official national registries. The most important responsibilities of this Central Office are to issue official documents (such as ID cards and passports) and to provide data for public administration authorities and citizens. The Central Office operates and supports the most significant electronic services for the public administration, and maintains the official governmental website and many other web pages for public services. It also provides ICT support for the authorities during elections and referendums.[14]

The state owned **National Infocommunications Service Company Ltd.** is responsible for ICT infrastructure development and maintenance for public administration. This company delivers, operates and supports the ICT infrastructure in the public administration.[15]

The most important e-Government service in Hungary is the Client Gate.[16] This is a website based, centralised electronic administration tool, where users can find and download the most frequently used electronic forms. The citizens can communicate with various authorities via the Client Gate. The website provides more than two thousand electronic forms[17] (tax declaration, healthcare, social status, company registry forms, etc.) and more than 80 different types of procedures.[18] As of 2015, the Client Gate has more than two million registered users.

Other essential e-Government solutions are the e-Company Registry,[19] e-Justice, and the authenticated electronic form of the Hungarian Official Journal.[20] The Standardised Central File and Document Management System is also a crucial e-Government tool in Hungary. It enables different ministries and other legal authorities to exchange files and electronic documents in an authenticated and digitally signed way.[21]

Thanks to these various e-governance solutions, Hungarian citizens' use of e-Government services was 49% in the last 12 months that ranked Hungary to the 16th place among EU 28 countries.[22]

---

[12] EU Digital Agenda, 'Country Ranking Table, On A Thematic Group of Indicators — Digital Agenda Scoreboard', 2014. <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"bbquality","ref-area":"HU","time-period":"2014"}>.
[13] eGovernment in Hungary. <http://eugo.gov.hu/key-facts-about-hungary/egovernment-hungary>.
[14] The Central Office for Administrative and Electronic Public Services. <http://www.kekkh.gov.hu/en/scope_of_duties>.
[15] National Infocommunications Service Company Ltd. <http://www.nisz.hu/en/about_us>.
[16] Client Gate. <https://ugyfelkapu.magyarorszag.hu>.
[17] Client Gate – Visiting Data. <https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html>.
[18] eGovernment in Hungary. <http://eugo.gov.hu/key-facts-about-hungary/egovernment-hungary>.
[19] e-Company Registry. <http://www.e-cegjegyzek.hu>.
[20] Hungarian Official Journal. <www.magyarkozlony.hu>.
[21] eGovernment in Hungary. <http://eugo.gov.hu/key-facts-about-hungary/egovernment-hungary>.
[22] EU Digital Agenda, 'Country Ranking Table, On A Thematic Group of Indicators — Digital Agenda Scoreboard', 2014. <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"egovernment","ref-area":"HU","time-period":"2014"}>.

1.2.2. E-commerce and e-business

Gradual development and long term of growth have been observed in e-Commerce in Hungary over the last 3-5 years. Turnover of HUF 273 billion (approximately €910 million) was realised in the e-Commerce sector in 2014, which amounted to an increase of 26% compared with the previous year.[23] However, the turnover of e-Commerce was only 3.7% of total commerce.[24] Individuals ordering goods or services online amounted to 32% of the population – which puts Hungary to 20th position in the EU – and 42% of internet users in 2014 which is also 20th place among the EU28.[25]

The turnover from e-Commerce was 32% among large enterprises (3rd place in the EU), but it only 7% from e-Commerce of SMEs (only 16th place in EU).[26]

2. Strategic national cyber security objectives

2.1. National cyber security foundation

Hungary is among the first countries in Central Europe to formulate its cyber security strategy, which focuses on a unique model of cooperation between state and non-state actors.[27] The *National Cyber Security Strategy of Hungary* (NCSS)[28] was adopted in 2013, enacted by Government Decision No. 1139/2013. The document is based on the foundations of EU and NATO cyber security principles and follows the mainstream take on cyber security strategies (values, environment, objectives, tasks, and tools). The document uses a comprehensive approach: it declares cooperation between state and non-state actors; military and law enforcement; and economic and political stakeholders.[29] Beyond analysing the cyber environment and clarifying the priorities, the NCSS also provides for the establishment of the highest political coordination body, the **National Cyber Security Coordination Council** (see section 3.1).

One year after the adoption of the NCSS, the draft of *National Cyber Security Action Plan* was finalised by the relevant working groups, but the Plan itself has not yet been officially adopted. The document was prepared with the involvement of governmental officials and private sector experts. The Plan focuses on the following main areas: organising the coordination of operational work; building and managing international relations; research and development; improving governmental IT projects; and education.

2.2. National cyber security objectives and priorities

According to the National Cyber Security Strategy: 'to promote the free and secure use of the cyberspace, Hungary declares the following objectives, to be achieved by aligning the interests of national security, efficient crisis management and user protection':

---

[23] eNet. 'Hungarian e-commerce volume hits all-time high'. <http://www.enet.hu/news/hungarian-e-commerce-volume-hits-all-time-high/?lang=en>.
[24] ibid.
[25] EU Digital Agenda, 'Country Ranking Table, On A Thematic Group of Indicators — Digital Agenda Scoreboard', 2014. <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"ecommerce","ref-area":"HU","time-period":"2014"}>.
[26] ibid.
[27] Réka Szemerkényi and Ferenc Suba, 'Public Private Partnership in Cybersecurity – The Hungarian Cooperative Model and Experience' *Cyber Security Review* Summer Issue (2014): 28.
[28] 1139/2013 (21 March) Government Decision on the National Cyber Security Strategy of Hungary. <http://www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx>.
[29] Suba Ferenc, 'Nemzeti Kiberbiztonsági Stratégia,' in *A nemzetbiztonság általános elmélete*, ed. Dobák Imre (Budapest: Nemzeti Közszolgálati Egyetem, 2014), 112. <https://opac.uni-nke.hu/webview?infile=&sobj=8964&source=webvd&cgimime=application%2Fpdf%0D%0A>.

1) *Building response capability:* having efficient capabilities to prevent, detect, manage (respond to), address and correct any malicious cyber activity, threat, attack or emergency, as well as accidental information leakage. To achieve these goals, the very first step was to establish the **GovCERT-Hungary**.

2) *Creating a secure environment:* providing appropriate protection for its national data assets, to ensure the operational safety of the cyberspace functions of its vital systems and facilities, and to have a sufficiently fast, efficient, loss-minimising correction system in situations where a compromise occurs, which can also be used at times of a special legal order (i.e. emergency situations).

3) *Applying international standards:* ensuring that the quality of IT and communication products and services required for a secure operation of the Hungarian cyberspace reaches international standards, with special emphasis on compliance with international security certification standards.

4) *Improving education:* ensuring that the standard of cyber security education, training and research and development is consistent with international best practices, promoting the establishment of a world-class Hungarian knowledge base. The government declared a significant role for the National University of Public Service in this matter, operating as the main base of education, training and research in the field of information security.

5) *Protecting the future generation:* ensuring that the establishment of a secure cyberspace for children and future generations is consistent with international best practice.

The strategy sets the priorities as the following: 'To meet present and future challenges, the strategy stipulates the requirement that the Hungarian cyberspace shall provide a secure and reliable environment:

- for individuals and communities, to ensure social development and integration through free and secure communication guaranteeing the protection of private information,
- for individuals and communities, to ensure social development and integration through free and secure communication guaranteeing the protection of personal information,
- for economic actors, to develop efficient and innovative business solutions,
- for future generations, to ensure value-based education and the collection of experience resulting in healthy, undisturbed mental development,
- for electronic public administration, to promote the innovative and future-oriented development of public service.'

2.3. National policies and legal acts on cyber security

Hungary's National Security Strategy[30] was drafted by the **Ministry of Foreign Affairs** and adopted by the Government in 2012. The Strategy was the third of its kind since the 1989 regime change and the first to address cyber security at such high level. The document highlighted the fact that 'the unhindered proliferation of the results of scientific and technological development and their potential malicious use by state or non-state actors, and even terrorist groups, to interfere with the normal operation of IT and communications systems and core governmental networks constitute an additional threat'; therefore, the capabilities of Hungary to respond to threats of these kinds have to be kept up-to-date and at readiness.

[30] 1035/2012 (21 March) Government Decree on the Hungary's National Security Strategy. <http://www.ecfr.eu/page/-/Hongrie_-_2012_-_National_Security_Strategy.pdf>.

The legal framework of most of the Hungarian cyber security organisations was founded by the *Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies*, and it was the first legal act based on the National Cyber Security Strategy.[31] Beyond the National Cyber Security Strategy, Act L of 2013 became the second main pillar to deal with the cyber defence structure.[32]

The provisions of the Act are quite wide and applicable to:

- constitutional and central state administration bodies, except for the Government and Government Committees;
- the offices of the representative bodies of local and nationality governments and the administrative associations of the authorities; and
- the Hungarian Defence Forces.

In accordance with the law, these governmental organisations and bodies have to reach different security institutional levels in information security. It means that these stakeholders should be categorised on a five point scale from level 1 to level 5. These levels, depending on the tasks and importance of the organisation, require different security personnel, measures and documents (e.g. IT security officers, log analysis, permanent vulnerability testing). Level 5 organisations have the most strict criteria. The latest guide to declaring these levels is the *Executive Decree of the Minister of Interior 41/2015 (15 July)*.

3. Cyber Security Organisational Structure

3.1. Political and strategic management, national and international cyber policy coordination

Political coordination and management are key elements of a nation's digital economy, developed information infrastructures and of course, cyber security. In the age of global alliances, 'digital power gives a clear asymmetric advantage in national security to small states',[33] of which Hungary is an example. Besides national coordination, international cooperation is the other main requirement of cyber security: 'Cyber defence is a cooperative effort, where no one, however powerful, can go it alone. You cannot build fences that are high enough to keep cyber threats away'.[34] Following this reasoning, the Hungarian Government has built up a complex cyber security system in recent years, focusing on the national and international environment and involving the private sector.

The **National Cyber Security Coordination Council**, created by the National Cyber Security Strategy, is the highest political coordination body in Hungary in this regard. The members of the Council are the ministerial leaders delegated by the ministers with responsibilities in the field of cyber security matters – including State Secretaries of Defence, Interior, Foreign Affairs and Trade, Finance, National Development – together with the heads of independent public entities, such as the Hungarian National Bank, and the National Media and Telecommunications Authority.[35] The Council operates under the supervision of the Ministry of Interior. The daily operative work is executed by the national cyber coordinator, who is coordinating the connected Cyber Security Working Groups (e.g. Homeland Security, Child protection, e-Government) as well, with the support of

[31] The Act L of 2013 also referred as 'information security law' or 'cyber law'.
[32] Krasznay Csaba and Török Szilárd, 'Hungary's Cyber Defense Readiness from the Perspective of International Recommendations,' *Hadmérnök* 1 (2014): 210. <http://hadmernok.hu/141_20_krasznaycs.pdf>.
[33] Liina Areng, 'Liliputian States in Digital Affairs and Cyber Security,' *The Tallinn Papers* 4 (2014): 11. <https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf>.
[34] Christian-Marc Liflander, 'Defining Cyber-Security: The Role of NATO in Ensuring Common Defence,' *Magyar Rendészet* Special Issue (2013): 138. <http://www.bm-tt.hu/assets/letolt/t2konf/MR_2013_KSZ_beliv.pdf>.
[35] Szemerkényi and Suba, 'Public Private Partnership in Cybersecurity,' 30.

senior experts. All the groups are co-chaired by a governmental official and a private expert. The working groups are a great example of how to involve the private sector into governmental decision-making.

The **National Cyber Security Forum** is another body of the Council, giving the opportunity for business CEOs, academic and NGOs' leaders to meet with governmental decision makers. Through the Forum, the non-state sector could become an active partner with the government during the legislative process. Moreover, national and international companies hold great knowledge and experience in the field of cyber security, which should be shared.

Operating under the Ministry of Interior, the **National Security Authority** promotes the protection of classified information and electronic systems that handle sensitive data. In accordance with Hungarian information security law – mentioned Act L of 2013 – from 1 July 2013 to the summer of 2015, the Authority was also responsible for the vulnerability assessments of governmental systems according to the National Electronic Information Security Authority requests.[36]

The Hungarian information security law created its assessment and supervision agency, the **National Electronic Information Security Authority**, which operates under the supervision of the Ministry of Interior. The dedicated main task of the Authority is to handle and control the data of central and local government agencies regarding their cyber security policies and declared security institutional level stipulated by confidentiality, integrity and availability.

Reflecting the intensive progression in cyber security matters, the first reform of Act L of 2013 took place in July 2015, two years after its adoption. Under the renewed system, the **Ministry of Interior** became responsible for the Hungarian cyber security direction and regulation. In accordance with the legislative amendment, to make the cyber defence system more united and centralised, **GovCERT-Hungary** became the main agency authorised to get involved in central governmental incident management. As another new element, in some cases, Act L of 2013 provides a basis for business sector companies (with a valid national security certificate) to take part in incident handling processes.

3.2. Operational cyber security capabilities, cyber incident management and coordination

The core operational cyber security capabilities and cyber incident management are centralised to the governmental computer emergency response team in Hungary, **GovCERT-Hungary**, which is part of the newly established National Cyber Defence Institute and supervised by the Ministry of Interior. GovCERT-Hungary provides services for the whole Hungarian governmental administration – especially for the government backbone system and for critical infrastructures – and the municipalities.[37]

GovCERT-Hungary started to operate on 1 July 2013. It has nearly 4,000 institutions as partners, and contributes to the protection of critical infrastructure with the National Directorate General for Disaster Management. GovCERT-Hungary has growing capabilities in the following fields: information exchange, sharing, publishing, information security awareness campaigns, training, technology watch, security consultancy, cyber incident response, coordination, resolution, basic malware analysis, manual analysis of system and firewall logs, source code validation, forensic examinations, and network traffic evaluation.[38] It is tasked with liaising with the private sector for the purposes of promoting information exchanges and raising awareness in the field of information and network security in the private sector. As a national contact point, GovCERT-Hungary builds active cooperation within the international CSIRT and CIIP community.[39] GovCERT-Hungary participates in

[36] In 2011, the Cyber Defence Management Authority (CDMA) was established within the Authority to be a national coordination and contact point to the NATO CDMA. It's operated within the National Security Agency until July 2015.
[37] GovCERT-Hungary. <http://www.cert-hungary.hu/en/node/17>.
[38] ibid.
[39] GovCERT-Hungary. <http://www.cert-hungary.hu/en/node/6>.

national and international cyber defence and crisis management exercises on regular basis. The agency also provides educational materials and holds training sessions for their constituents.[40]

The near-term goals of GovCERT-Hungary are to develop and establish full scale, dynamic malware analysis, automated log analysis, higher event correlations, and remote examinations. Other aims are to create an online malware and knowledge database and to establish a cyber-alert early warning system.[41]

To ensure cooperation and the flow of information on higher levels on a daily basis, the **National Cyber Defence Institute** was established on 1 October 2015. The institute operates as an umbrella organisation, incorporating the GovCERT-Hungary, the National Electronic Information Security Authority and the Cyber Defence Management Authority.[42] The goal is to make task execution and incident handling processes more coordinated and efficient. The institute also serves as a contact point in several international forums, such as Forum of Incident Response and Security Teams, International Watch and Warning Network, and European Government CERTs Group, using the existing knowledge base coming from the cyber security organisations.

Sectorial CERTs are also being established: beyond the existing critical information infrastructure protection (CIIP) CERT (operating under the National Directorate General for Disaster Management), another two are being set up, one for defence within the Military National Security Service, and another one for civilian intelligence within the Information Office.

3.3. Military cyber defence

In 2012, the Government adopted *Hungary's National Military Strategy*.[43] This strategy was the first official declaration of Hungary considering cyberspace as the fifth domain. According to the document, the **Hungarian Defence Forces** (HDF) are facing threats not just from the physical dimension but from cyberspace as well, and preparing to wage a new type of war. It concludes, 'The characteristics of cyber threats which are different from those of conventional threats necessitate a comprehensive review and possible amendment of our concepts of war'.

The political and military leaders had to face the fact that 'nations today use computer network operations to defend sovereignty and to project power, and cyber conflicts may soon become the rule rather than the exception'.[44]

This point of view has become a standard NATO approach, following the declaration at the Chicago Summit, 2012, that cyber capabilities are vital to achieve military goals in today's wars.[45] However, NATO is still rather cautious about drawing an equation mark between cyber capabilities and military capabilities. Moreover, according to the Wales Summit Declaration, 2014, 'a decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.'[46]

[40] Szentgáli Gergely, 'A magyar kibervédelem anatómiai képe, ' *Felderítő Szemle* 3 (2013): 80. <http://knbsz.gov.hu/hu/letoltes/fsz/2013-3.pdf>.
[41] Balázs Bencsik: GovCERT-Hungary - Vision and Strategy. <http://konferencia.infoter.eu/_dwl/D%C3%ADszterem/7/1405-1420%20-%20dr.%20bencsik%20bal%C3%A1zs.pdf>.
[42] The organisational design of the Institution follows a model also used in Germany (Federal Office for Information Security) and in the Netherlands (National Cyber Security Centre).
[43] 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>.
[44] Kenneth Geers, 'Pandemonium: Nation States, National Security, and the Internet,' *The Tallinn Papers* 1 (2014): 12. < https://ccdcoe.org/publications/TP_Vol1No1_Geers.pdf>.
[45] Szentgáli Gergely, 'NATO Policy on Cyber Defence: The Road so Far,' *AARMS* 1 (2013): 87. <http://uni-nke.hu/uploads/media_items/aarms-vol-12_-issue-1_-2013.original.pdf>.
[46] Wales Summit Declaration. <http://www.nato.int/cps/en/natohq/official_texts_112964.htm>.

In 2013, the Ministry of Defence issued the *Cyber Defence Concept of the Hungarian Defence Forces*.[47] This concept outlines the main directions for the HDF and defines general requirements of the cyber security task required of the HDF and their organisations. In order to create and develop the cyber defence capabilities of the HDF the document assigns a three-level development plan, which includes initial cyber defence capabilities (2013-2014), basic cyber defence capabilities (2013-2016), and full cyber defence capabilities. These capabilities will build on full network security perspective, which will include network monitoring, military CSIRT capabilities, and cyber security of tactical and operational networks.

Besides the core cyber defence capabilities, the document emphasises the needs for development of the legal and regulatory environment, raising the level of security of electronic data management networks, application of certified products, increasing security awareness and knowledge, cyber security research and development, and cooperation between stakeholders.

In late 2014, the Minister of Defence ordered the **Military National Security Service** to set up and continue to develop the Computer Incident Response Capability (MilCIRC) and afterwards to establish a Military Computer Emergency Response Team (MilCERT).[48]

The MilCIRC cooperates with GovCERT-Hungary in incident handling, and is authorised to perform vulnerability tests in the military defence sector.[49] MilCIRC is going to be an umbrella organisation incorporating the main stakeholders of defence sector.

In accordance with the Constitution, the MoD has responsibility only for security of military communications in peacetime. The **Communications, Information Systems and Information Security Directory of the Hungarian Defence Forces General Staff** has basic management functions for operating and security issues of military networks and a coordination role with governmental organisations, authorities and other partners including NATO and EU cooperation.

The HDF has its own military communication and information system (CIS), the HDF Network (HDFN) for supporting the activities of all military organisations from strategic to tactical levels, including cooperation with partners and NATO organisations. Under the control of the CIS and CIS Security Directorates, the IT Centre of the Budapest Garrison Brigade has basic network management functions of HDFN including security mechanisms and elements. HDFN security incident handling capability (HDF CIRC) will be improved according to the requirements of the mentioned Concept in line with government and NATO requirements.

Hungary joined to the NATO CCD COE as a Sponsoring Nation in June 2010. The country contributes to the main aims of the Centre of Excellence and participates to enhance the cyber defence capability, cooperation and information sharing within NATO. Hungary places great emphasis on education, research and development, and consultation within the CCD COE.

3.4. Crisis prevention and crisis management

On 1 January 2012, a new disaster management law was adopted by *Act CXXVIII of 2011* in Hungary. This law set three main pillars for disaster management: fire protection, civil protection, and industrial safety. The **National Directorate General for Disaster Management** (NDGDM), supervised by the Ministry of Interior, is the key player in these fields. Its main mission is preventing disasters as an authority, organising and controlling

[47] 60/2013 (30 September) Minister of Defence decree on Cyber Defence Concept of Hungarian Defence Forces. <http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/10.pdf>.

[48] 85/2014 (23 December) Minister of Defence decree on the main objectives and key tasks of national defence organisations for 2015, and determining the main directions of activity of the years 2016-2017. <http://www.kozlonyok.hu/kozlonyok/Kozlonyok/12/PDF/2014/64.pdf>.

[49] 185/2015. (VII. 13.) Gov. decree about scope of the governmental incident handling centre and incident handling centre's duties and their sphere of action, and about the rules of handling of security incidents, technical investigation of security incidents and penetration testing. <http://njt.hu/cgi_bin/njt_doc.cgi?docid=176703.296223 >

protection activities, carrying out rescue operations in civil emergencies, eliminating the negative consequences of emergencies, and executing and contributing to reconstruction and recovery.[50]

There is an unambiguous connection between cyber security and critical infrastructures and NDGDM plays a definite role in the protection of these infrastructures as well. The most recent legislation in this field is *Act CLXVI of 2012 on the Identification, Designation and Protection of Vital Systems*. Hungary follows the critical infrastructure concept set out in the EU Directive[51] and has identified ten vital sectors: energy, transport, water, ICT, finance, agriculture, industry, public health, government, public security and defence management.[52] The execution of *Government Decree 65/2013 (8 March)* followed on identification and designation of critical systems and facilities.[53] According to these regulations, and based on Act L of 2013, a **Critical Infrastructure Cyber Incident Response Centre** was established within the framework of the National Inspectorate General of Industrial Safety of NDGDM. The main missions of the Centre are ensuring and contributing to network security of critical infrastructure elements, treatment of industrial security incidents, training, and participating in industrial and network security exercises. The Centre is involved in the development work of strategies for protection of critical information and electronic systems and preparation of regulators for the protection of industrial facilities.[54] The Critical Infrastructure Cyber Incident Response Centre coordinates response actions and cooperates with the GovCERT-Hungary in case of industrial security incidents.

[50] National Directorate General for Disaster Management: Introduction. <http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_intro&lang=eng>.
[51] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>.
[52] Kadri Kaska and Lorena Trinberg, *Regulating Cross-Border Dependencies of Critical Information Infrastructure* (Tallinn: NATO CCDCOE, 2015), 39. <https://ccdcoe.org/sites/default/files/multimedia/pdf/CII_dependencies_2015.pdf>.
[53] 65/2013 (8 March) Government Decree on identification and designation of critical systems and facilities. <http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300065.KOR>.
[54] Balázs Bognár: Identification and designation process of critical infrastructures. The results of the LRL IBEK operation. NDGDM expectations regarding the training of the NUPS. <http://vtki.uni-nke.hu/downloads/tk/IBOT_PILOT/PLENARIS/Dr_Bognar_Balazs.pdf>.

References

1035/2012 (21 March) Government Decree on the Hungary's National Security Strategy. <http://www.ecfr.eu/page/-/Hongrie_-_2012_-_National_Security_Strategy.pdf>

1139/2013 (21 March) Government Decision on the National Cyber Security Strategy of Hungary. <http://www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx>

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>

185/2015. (13 July) Gov. decree about scope of the governmental incident handling centre and incident handling centre's duties and their sphere of action, and about the rules of handling of security incidents, technical investigation of security incidents and penetration testing. <http://njt.hu/cgi_bin/njt_doc.cgi?docid=176703.296223 >

60/2013 (30 September) Minister of Defence decree on Cyber Defence Concept of Hungarian Defence Forces. <http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/10.pdf>

85/2014 (23 December) Minister of Defence decree on the main objectives and key tasks of national defence organizations for 2015, and the main directions of activity of the year determining the on 2016-2017. <http://www.kozlonyok.hu/kozlonyok/Kozlonyok/12/PDF/2014/64.pdf>

Balázs Bencsik: GovCERT-Hungary - Vision and Strategy. <http://konferencia.infoter.eu/_dwl/D%C3%ADszterem/7/1405-1420%20-%20dr.%20bencsik%20bal%C3%A1zs.pdf>

Client Gate – Visiting Data. <https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html>

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>

Christian-Marc Liflander, 'Defining Cyber-security: The Role of NATO in Ensuring Common Defence' *Magyar Rendészet* Special Issue (2013): 137-139. <http://www.bm-tt.hu/assets/letolt/t2konf/MR_2013_KSZ_beliv.pdf >

Digital Renewal Action Plan. <http://infoter.eu/alapdokumentumok/digitalis_megujulas_cselekvesi_terv>

GovCERT-Hungary.

<http://www.cert-hungary.hu/en/node/6>

<http://www.cert-hungary.hu/en/node/17>

eGovernment in Hungary. <http://eugo.gov.hu/key-facts-about-hungary/egovernment-hungary>

eNet. Hungarian e-commerce volume hits all-time high. <http://www.enet.hu/news/hungarian-e-commerce-volume-hits-all-time-high/?lang=en>

EU Digital Agenda, 'Country Ranking Table, On A Thematic Group of Indicators — Digital Agenda Scoreboard', 2014. <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators>

Hungarian Information Society Strategy, Budapest 2003. Cited in 'Report on Hungarian Information Society 1998-2008'. <http://infoter.eu/attachment/0003/2817_ittk_mitj_1998_2008.pdf>

Hungarian Central Statistical Office: Statistic Mirror. 43/2015. <http://www.ksh.hu/docs/hun/xftp/gyor/tav/tav1503.pdf>

Kadri Kaska and Lorena Trinberg, *Regulating Cross-Border Dependencies of Critical Information Infrastructure* (Tallinn: NATO CCD COE, 2015) <https://ccdcoe.org/sites/default/files/multimedia/pdf/CII_dependencies_2015.pdf>

Kenneth Geers, 'Pandemonium: Nation States, National Security, and the Internet,' *The Tallinn Papers* 1 (2014) <https://ccdcoe.org/publications/TP_Vol1No1_Geers.pdf>

Krasznay Csaba and Török Szilárd, 'Hungary's Cyber Defense Readiness from the Perspective of International Recommendations' *Hadmérnök* 1 (2014): 209-216. <http://hadmernok.hu/141_20_krasznaycs.pdf>

Liina Areng, 'Liliputian States in Digital Affairs and Cyber Security' *The Tallinn Papers* 4 (2014) <https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf>

Ministry of National Development: National Info-communication Strategy: Fully electronic services in public administration within four years. <http://2010-2014.kormany.hu/en/ministry-of-national-development/news/national-info-communication-strategy-fully-electronic-services-in-public-administration-within-four-years>

National Directorate General for Disaster Management: Introduction. <http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_intro&lang=eng>

National Info-communication Strategy. <http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf>

National Information Society Strategy, Budapest 2001. Cited in 'Report on Hungarian Information Society 1998-2008'. <http://infoter.eu/attachment/0003/2817_ittk_mitj_1998_2008.pdf>

Réka Szemerkényi and Ferenc Suba, '*Public Private Partnership in Cybersecurity – The Hungarian Cooperative Model and Experience*' *Cyber Security Review* Summer Issue (2014): 28-32.

Suba Ferenc, 'Nemzeti Kiberbiztonsági Stratégia,' in *A nemzetbiztonság általános elmélete*, ed. Dobák Imre (Budapest: Nemzeti Közszolgálati Egyetem, 2014), 110-115. <https://opac.uni-nke.hu/webview?infile=&sobj=8964&source=webvd&cgimime=application%2Fpdf%0D%0A>

Szentgáli Gergely, 'A magyar kibervédelem anatómiai képe, '*Felderítő Szemle* 3 (2013): 74-89. <http://knbsz.gov.hu/hu/letoltes/fsz/2013-3.pdf>

Szentgáli Gergely, 'NATO Policy on Cyber Defence: The Road so Far,' *AARMS* 1 (2013): 83-91. <http://uni-nke.hu/uploads/media_items/aarms-vol-12_-issue-1_-2013.original.pdf>

Wales Summit Declaration. <http://www.nato.int/cps/en/natohq/official_texts_112964.htm>