CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Lea Hriciková and Kadri Kaska

National Cyber Security Organisation: Slovakia

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Italy

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in the USA

Upcoming in 2015

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Lithuania

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 November 2014.

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 competence, as well as 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 Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the USA as Sponsoring Nations. 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.

SLOVAKIA

By Lea Hriciková
Visiting Fellow, NATO CCD COE

and Kadri Kaska
Researcher, NATO CCD COE

1. Introduction: information society in Slovakia

The development of information society in Slovakia has been a mixture of an organic effort and the country's ambition to play a confident role in international organisations.

In 2001, the Slovak government adopted the first *Information Society Policy of the Slovak Republic*, which declared the Government's strategic intent to develop an information society. The strategy was followed up by the 2004 Information Society Strategy and an accompanying Action Plan outlining long-term priority areas (in infrastructure, content, and human resources) together with specific tasks and a timetable. The plan was flexible to accommodate developing needs and its implementation was continuously monitored; however, it was criticised for lacking adequate funding. The subsequent Information Society Strategy for 2009-2013 built upon the experience of its predecessor, while taking into account the ongoing economic crisis. Considering the slow growth of the ICT sector, Bratislava pursued stronger engagement in six key areas: broadband deployment, information security, e-government, e-health, digital literacy, and energy efficiency.[1] To this end, the Ministry of Finance of the Slovak Republic, in collaboration with the Government Plenipotentiary for Information Society, is the designated coordinator for information society in the state administration.[2]

In addition, other national strategy documents have supported information society development, including the Competitiveness Strategy for the Slovak Republic until 2010 (adopted in 2005 as the Slovak Government's reaction to the EU Lisbon Strategy), two National Reform Programmes (2006-2008 and 2008-2010),[3] and the Sustainable Development Action Plan for 2005–2010.[4] The national Operational Programme Information Society has supplied funding and measures in four priority areas: making electronic services available at the local, regional and national level; building electronic repositories of digital data and a national capacity for the management and protection of digital data; improving the availability of broadband access infrastructure; and technical services.[5] The implementation of the Competitiveness Strategy in connection with the Information Society Action Plan resulted in several successful projects.[6]

1.1. Infrastructure availability and take-up

By 2013, standard fixed broadband was available to merely 85% of the Slovak households, which was the lowest figure in the EU.[7] 58% of households were located in areas serviced by high speed Next Generation Access networks.

Against this background, the demand for Internet access appears fairly active, with the number of households with broadband connections on a steady rise. 78% of households in Slovakia had some form of access to the internet at home; the majority of those – 70% of all households – held a broadband connection. Both of these figures compare to the EU average. Among enterprises, take-up amounts to is 87% (EU 20th).

Basic broadband speed of at least 2 Mbps amounts to 96% of fixed broadband subscriptions; 26% of subscriptions reach a speed of at least 30Mbps and 8% of 100Mbps (2013), which roughly corresponds to the European average, ranking 20th, 13th and 9th respectively.

---

[1] The Ministry of Finance of the Slovak Republic, 'Information Society Strategy for 2009–2013', Bratislava, 2009, 6-16 <http://www.informatizacia.sk/ext_dok-information-society-startegy-for-2009_2013/6497c>.
[2] ibid, 4.
[3] The two documents were approved by Government Resolution No. 522/2001 and by Government Resolution No. 43/2004 on 21 January 2004. ibid, 4-6.
[4] ibid.
[5] ibid, 16; Office of the Government of the Slovak Republic, 'Operational Programme Informatisation of Society', Version 4.0, Bratislava, 2012 <http://www.opis.gov.sk/data/files/2448_8949.pdf>.
[6] Information Society Strategy (n **Error! Bookmark not defined.**) 5.
[7] Unless otherwise indicated, statistical data in this section is drawn from the *EU Digital Agenda Scoreboard* for Slovakia in 2013. See: EU Digital Agenda, 'Country Ranking Table, On A Thematic Group Of Indicators — Digital Agenda Scoreboard' <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"egovernment","ref-area":"SK","time-period":"2013"}>.

Regular Internet users amounted for 74% of the population (13th position in the EU).

The rural areas are unattractive to private sector broadband service providers due a slow return on investment and high associated business risk, and are consequently dependent on state subsidies such as the Operational Programme Information Society (OPIS) to develop broadband access networks. A broadband access strategy was defined in the National Policy for Electronic Communications for 2009-2013 and the National Broadband Strategy of the Slovak Republic (adopted in 2011 with no expiration date) under the auspices of the Slovak Ministry of Transport, Posts and Telecommunications.[8] Infrastructure development remains supported by a state aid measure until the end of 2015, but further aid is planned beyond that date to bring broadband coverage to speeds above 30 Mbps for the entire population by 2020.[9] Legislative measures also appear to be underway to simplify the building of networks and introduce access and price regulation in an effort to stimulate competition while optimising profitability to protect investment.[10]

1.2. E-government and private sector e-services

In 2010, Slovakia had the third least available e-government for its citizens with only 46% of key public services available online. Citizens' use of the e-Government has been in a constant decline, dropping from 50% to 33% between 2010 and 2013, translating into a drop from 8th position among EU countries to 20th.[11] The online availability of basic public services for enterprises reached 88% in 2010); 92% of all enterprises made use of these services in 2013, which, regardless of a usage decline, ensures Slovakia a position above the European average.

The share of e-commerce in Slovakia amounted to 3.3% of the country's GDP in 2011.[12] In terms of e-business services, Slovak large enterprises lag behind the European benchmark in integrating internal processes, but the gap between large and small businesses is less pronounced in Slovakia due to the above-average performance of Small and Medium Enterprises (SMEs) in this area (68% of large enterprises and 31% of SMEs). Slovak enterprises are among the EU top five in sending and receiving e-invoices (43%) and using electronic supply chain management (55% of large enterprises and 39% of SMEs in 2012) at 5th, 5th and 4th places respectively. With regards to outreach, 55% of Slovak enterprises use automated data exchange with other ICT systems outside their own enterprise.[13] In addition, 80% of Slovak enterprises have a dedicated website, which correlates strongly with the metric that over half of Slovak internet users (55%) order goods or services online.

A fifth of all internet users engage in cross-border e-commerce, which has afforded Slovakia the third highest turnover[14] from e-commerce for SMEs (10%) and fifth highest turnover for large enterprises (24%) in the EU. In 2010 Slovakia had the 7th biggest ICT sector in Europe[15] and the estimated added value of the sector was 33.8%, the highest in Europe.[16] However, the sector is predominantly focused on manufacturing goods as opposed to services.

---

[8] Information Society Strategy (n **Error! Bookmark not defined.**) 8, 10. Now the Ministry of Transport, Construction and Regional Development.
[9] European Commission, 'Country Information - Slovak Republic', 2014 <http://ec.europa.eu/digital-agenda/en/country-information-slovak-republic>.
[10] ibid.
[11] Eurostat, 'Benchmarking Digital Europe: Key Performance Indicators', 2014 <http://ec.europa.eu/eurostat/web/employment-and-social-policy/information-society/indicators>. (*Public Service – Individuals).*
[12] See a study commissioned by Google: The Boston Consulting Group (BCG), 'Slovakia Online - How the Internet Is Transforming the Slovak Economy', 2012 <http://www.onlinesanca.sk/pdf/BCG_Google%20Slovakia%20Online_EN.pdf>.
[13] Eurostat, 'ICT Usage by Enterprises, Integration with customers/suppliers and SCM' <http://ec.europa.eu/eurostat/help/new-eurostat-website>.
[14] Ecommerce amounts for 13% of total turnover in 2009. Eurostat <http://ec.europa.eu/eurostat/help/new-eurostat-website>.
[15] Eurostat, 'ICT Sector, Percentage of the ICT Sector on GDP' <http://ec.europa.eu/eurostat/help/new-eurostat-website>.
[16] Eurostat, 'ICT Sector, Percentage Change of Value added by ICT Sector at Current Prices' <http://ec.europa.eu/eurostat/help/new-eurostat-website>.

Overall, and unlike the rest of Europe, policy relating to information society building in Slovakia has not yet shifted away from infrastructural issues, which are still predominant, to socio-economic goals. Slovakia still needs to support investment for service coverage but also improve the quality as well as the amount of services that government provides online for citizens as well as for enterprises. While national infrastructure remains important, increasingly the information society will not be possible without substantial investment in human capital and knowledge development, supported by strategic investment in the areas of education, science, research and innovation.[17]

2. Strategic national cyber security objectives

The central strategic document for cyber security is the *National Strategy for Information Security of the Slovak Republic* (NSIS) 2009–2013, enacted by Government Regulation No. 570/2008. The strategy was drafted by the Ministry of Finance of the Slovak Republic, which is the authority for information security pertaining to all unclassified information in public administration and the general public.[18]

2.1. National cyber security strategy

NSIS is the first document of its kind and only later have documents released by the Ministry of Defence and the Security Council of the Slovak Republic addressed cyber security. Among those are the annual *Report on the Security of Slovak Republic* in 2012 and the *White Paper on Defence of the Slovak Republic*.[19]

The NSIS is accompanied by the *2010 Action Plan* and the Report on the *Tasks of the NSIS and the Action Plan for 2009-2013* issued each year. The *Action Plan* directly connects the NSIS to the relevant strategic documents of the EU, as well as the interests of OECD and NATO policy but also clarifies deadlines, potential risks and the hierarchy of problem solution. The strategy will be financially supported by the EU OPIS.[20]

2.2. Cyber security strategy objectives

The NSIS identifies long-term strategic objectives of the Slovak Republic in information security. These are based on the EU strategic interest in economic growth and in promoting global cooperation. Thus, the focus is on the user who demands a level of security for digital products and services, as well as ensuring a competitive environment for online service providers. For this reason the NSIS focuses on standardisation and takes consideration for the legitimate interests of citizens, the business sector and public administration are taken into account. These objectives 'comply with the Slovak Security Strategy, approved by the National Council of the Slovak Republic in September 2005'.[21]

The objectives of the NSIS are:

---

[17] Information Society Strategy (n **Error! Bookmark not defined.**) 7, 9.

[18] Ministerstvo financií SR, 'Národná stratégia pre informačnú bezpečnosť v Slovenskej republike', 2008, 6 <http://www.informatizacia.sk/ext_dok-narodna_strategia_pre_ib/6167c> (in Slovak); The Ministry of Finance of the Slovak Republic, 'National Strategy for Information Security in the Slovak Republic (NSIS)', 2008, 6 <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf> (in English).

[19] National Strategy for Information Security (n 18) 8;
The Ministry of Defence of the Slovak Republic, 'The White Paper on Defence of the Slovak Republic', 2013, 49, 127 <http://www.mosr.sk/data/WP2013.pdf>; 'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2012, 4 para 7 <http://www.informatizacia.sk/ext_dok-sprava_2012_strategia_a_akcny_plan_ib/16200c>. [*Report on the Tasks Execution of the Action Plan for 2009-2013 for the National Strategy for Information Security in SR*, hereafter 'Report 2012'].

[20] 'Opatrenie - Akčný plán informačnej bezpečnosti', 4 <http://www.informatizacia.sk/ext_dok-akcny_plan_k_strategii_pre_ib/6790c>. [*Action Plan for the Information Security,* hereafter 'Action Plan'].

[21] National Strategy for Information Security (n 18) 8.

1. *Prevention*: for adequate protection of Slovak digital space so as to prevent the occurrence of security incidents;
2. *Readiness*: to ensure the ability to effectively respond to and mitigate the impact of security incidents, and restore the operation of information and communication systems after an incident;
3. *Sustainability*: to achieve, maintain and upgrade Slovakia's competence in information security.

The NSIS outlines strategic priorities, to which key tasks are assigned:[22]

1. *Protection of human rights and freedoms,* i.e. protecting the legitimate interests of all stakeholders involved in the use of ICT. This principle involves two aspects: democratic principles that must underwrite all measures designed to protect Slovak digital space, and the legal framework which ensures the proper protection of personal data.

Based on this strategic priority, amendments have been made to the Act No. 428/2002 Coll. on Protection of Personal Data and to the Penal Code Act No. 300/2005 Coll., which now incorporates the principles of the Council of Europe Convention on Cybercrime.[23] The share of organisations with updated personal data policies (no older than two years) had increased to 81 % by 2013.[24]

2. *Building awareness and competence in information security*, including awareness raising, strengthening education activities, and introducing programmes for enhancing security awareness and competence of ICT users. As a result, the 2009 *System of Education in Information Security in Slovak Republic* was the first government-approved document originating from the Strategy, and it aims to build-up of the culture of use of ICT. A systematic education of the public administration employees was set out in 2013.[25] The education of the general public is funded and carried out by the Ministry of Education, Science, Research and Sport through various projects. The transnational initiative *Government Security Program* (Government Resolution No. 310/2008) covers the education of experts in coordination with the CSIRT.SK, the Computer Security Incident Response Team Slovakia.[26]

3. *Creation of a secure environment*. This involves the creation of a sufficient legal framework which respects basic rights and freedoms as well as the international obligations of Slovakia and involves the private sector and academia in the legislative process. It also covers defining the responsibilities and competencies of the public administration and coordinating standardisation.

In 2010, the Government approved the *Legislative Intent of the Information Security Act* (Government Resolution No. 136/2010) that set up the structural baseline for information security and coordinates the needs and competencies of responsible agencies. The Act was scheduled to come into force in 2014.[27]

Furthermore, the fragmentation of competences, dual issuance of standards and their incompatibility were addressed in the amendments to the *Act on Information Systems of the Public Administration* (ISPA Act No. 275/2006) that make the issuance of standards subject to the approval of the Ministry of Finance. [28]

---

[22] National Strategy for Information Security (n 18) 9-13; Action Plan (n 20). The tasks for the forthcoming period found in NSIS pp. 17-20 are not as specific as the tasks outlined in the Action Plan, pp. 6-11, that are described here for this purpose.
[23] Council of Europe, 'Convention on Cybercrime', CETS No. 185, Budapest, 2001 <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>; for the exhaustive list of legislation in the information security legislative framework see: National Strategy for Information Security (n 18) Annex I.
[24] As revealed by a survey on the state of information security in 2013. Ministerstvo financií SR 'Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike v roku 2013', 2013, 5 <http://www.informatizacia.sk/prieskum-stavu-ib/12772s>.
[25] Report 2012 (n 19) 1.
[26] The CSIRT.SK (sometimes referred to as CSIRT.GOV) has taken part in the CESNET workshop, NATO CCD COE training events, ITU Regional Forum on Cybersecurity for Europe and CIS training, TERENA TRANSIT I. training, Web Application seminars, Linux seminars and ISO norms seminars. In Action Plan (n 20) 5-6.
[27] European Commission, eGovernment Factsheets, 'eGovernment in Slovakia', Edition 16.0, 2014, 16 <https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGov%20SK%20-%20April%2014-v_16_0.pdf>.

The Ministry of Finance has also conducted analyses of information security in the Slovak Republic (in 2009 and 2011) and has published a yearly survey on the state of information security in public administration since 2011.[29]

4. *Improving effectiveness in information security management.* This task involved the integration of the CSIRT into the European cooperation structures (ENISA, EP3R), increasing its preparedness in incident prevention, forming an information sharing system and warning mechanisms for the detection of threats and reaction to incidents, setting up interagency planning for incident management, and nation-wide exercises for moderation of the effects and post-incident recovery. CSIRT.SK (set up in 2009) joined ENISA in 2010 and was fully accredited by the Trusted Introducer into the TF-CSIRT in 2011. A computer laboratory for forensic analysis, penetration testing, malware and network analysis, and a system of information sharing, early warning and incident reaction known as *Thermis*, were created in 2012 and have been operational since 2013.[30]

5. *Ensuring sufficient protection of the critical (information) infrastructure.* The task envisaged identifying national critical infrastructure and ensuring its security by increasing the information security in state agencies, implementation of secure products, systems and conditions for introducing new measures. [31] As a result, the *Interdepartmental Programme for Financial Support of Measures for the Protection of Critical Infrastructure* took place in 2010[32] and *Act No. 45/2011 on Critical Infrastructure* proposed by the Ministry of Interior was enacted in 2011.[33] The elements of security in CI are subject to a review submitted by the Interior to the Security Council of Slovak Republic.[34]

6. *National and international cooperation* is mainly aimed at coordinating Slovakian national efforts in cyber security by effectively engaging in international cooperation based on national needs and priorities.

7. *Enhancement of national competence, including* an analysis of national qualification needs in information security, possibilities for relevant education and training, and the introduction of a training system as well as the promotion of research and development and supporting economic competitiveness.

3. National organisational structure for cyber security and cyber defence

3.1. Political and strategic-level cyber security management

The key to the organisational structure for cyber security and cyber defence in Slovakia is the distinction made between the management and information security of classified and unclassified information.[35] The former is

---

[28] Information Society Strategy (n **Error! Bookmark not defined.**) 12.

[29] 'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2009 <http://www.informatizacia.sk/ext_dok-sprava_2009_strategia_a_akcny_plan_ib/6788c>; 'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2011 <http://www.informatizacia.sk/ext_dok-sprava_2011_strategia_a_akcny_plan_ib/16198c> [hereafter 'Report 2011']; Report 2012 (n 19); 'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2013 <http://www.informatizacia.sk/ext_dok-sprava_2013_strategia_a_akcny_plan_ib/16201c> [hereafter 'Report 2013']; See also: Prieskum stavu informačnej bezpečnosti (n 24).

[30] Report 2013 (n 29) 2. The core of *Thermis* is a Security Information and Event Management (SIEM) monitoring system.

[31] Action Plan (n 20) 8-9.

[32] Report 2012 (n 19) 4. The programme includes the Ministry of Finance, the Ministry of Transport, Constructions and Regional Development, Ministry of Economy, Ministry of Health and the Ministry of Environment.

[33] Report 2011 (n 29) 4. The basis for the Act was the EC Directive 2008/114/EC. Slovenskej republiky, 'Zákon o kritickej infraštruktúre', Zbierka zákonov č. 45, 2011 <www.zbierka.sk/sk/predpisy/45-2011-z-z.p-33998.pdf>.

[34] Report 2013 (n 29) 6.

[35] National Strategy for Information Security (n 18) 13.

dealt with by the **National Security Authority** (NSA)[36]; the latter is under the supervision of the **Ministry of Finance**. Related areas are subject to sectoral legislation, which also outlines the responsibilities of specialised governmental agencies for these areas. For example, integrated crisis management and critical infrastructure protection is coordinated by the Crisis Management Section of the Ministry of the Interior.[37]

Mutual communication is facilitated by the Ministry of Finance's **Committee for Information Security**, which has an advisory and coordinating role, preparing 'strategic and technical materials on information security'.[38] The committee is composed of representatives from the Information Society Section of the Ministry of Finance, the Office of the Government, the Ministry of Interior, NSA, Slovak National Accreditation Service, IT Association of Slovakia, Slovak Association for Information Security, and a representative of an academic research institution in information security.

The **Ministry of Finance** provides input on the legislative process via the Legislation, Standards and Security of Information Systems Department. The Department belongs under the Information Society Section,[39] analysing various aspects including financial and business environment of the impact on information society development, according to the directive for material submission for government meetings. The Department represents the Ministry of Finance on matters of internet governance, standards, and information security in the Legislative Council of the Slovak Government, but also at the EU and other institutions. It oversees standards implementation in the public administration sector and its information systems.[40]

The **National Security Authority** is the main body of state administration for the protection of classified information and cryptographic services. The NSA fulfils tasks arising from Slovak membership of NATO and of the EU, providing protection for foreign classified information shared with the Slovak Republic in accordance with international agreements, and cooperates with national security authorities of other states and security authorities of international organisations. In accordance with Act No. 215/2004 Coll. on the Protection of Classified Information, its Department of Cyber Security creates conditions for information security under the Information Security and Electronic Signature Section, which is, apart from the Directorate, also subject to supervision of the agency's Auditor and Control Department.[41] The NSA is overseen by Special Parliamentary Control Committee for the Control of NSA Activities.[42]

Strategic documents for both, the NSA and the Ministry of Finance, are approved by the Government of the Slovak Republic which also oversees the fulfilment of the strategic tasks. Their management is subject to review by the Government's Security Council in its annual *Report on the Security of the Slovak Republic*. The Security Council has a mandate to initiate and coordinate the efforts of state security and provide advice on security matters to the Government and the President, in cooperation with ministries and other agencies of public administration. In practice, the Security Council discusses proposed security matters[43] and subsequently issues a resolution with binding tasks. The Security Council is entitled to obtain necessary information from the ministries and other central or local public administration agencies.[44] According to the *Working Programme of the Security Council of the Slovak Republic* for 2014, the Council is to consider the readiness of the Slovak

[36] Sometimes referred to as the National Security Office.
[37] See: Ministerstvo vnúra SR, 'Nenájdený dokument' <http://www.minv.sk/?sekcia_izs_km_mvsr>.
[38] The Ministry of Finance of the Slovak Republic, 'Information Security' <http://informatizacia.sk/information-security/4622s>; National Strategy for Information Security (n 18) 13.
[39] Ministerstvo financií SR, 'Kontakty' <http://informatizacia.sk/kontakty/4795s>.
[40] Sekcia informatizácie spoločnosti, 'Členenie a Pôsobnosť odborov/oddelení Sekcie informatizácie spoločnosti', 2008 <http://www.informatizacia.sk/sekcia-informatizacie-spolocnosti/5188s>.
[41] Národný bezpečnostný úrad (NBÚ), 'Štruktúra úradu' <http://www.nbusr.sk/sk/struktura-uradu.1.html>.
[42] National Security Authority (NBÚ), 'National Security Authority' <http://www.nbusr.sk/en/>.
[43] By the members of the council, Ministers, heads of public administration agencies, the representatives of local government and by its expert working groups.
[44] Office of the Government of the Slovak Republic, 'Statute of Security Council of Slovak Republic', Resolution No. 162, 28 February 2007, Art. 1-2, 6, 8 <http://www.government.gov.sk/statute-of-the-government-office-of-the-slovak-republic/?pg=2>; Úradu vlády SR 'Spoločný rokovací poriadok Bezpečnostnej rady kraja', 26. februára 2003, Čl. 3, 4 <http://www.vlada.gov.sk/spolocny-rokovaci-poriadok/>.

Republic for completing tasks in cyber defence. It also carries out tasks such as national preparations for the NATO Cyber Coalition exercise 2014 and, most importantly, drafting the cyber security strategy.[45]

Parliamentary oversight is executed through the Parliamentary Committee on Defence and Security which comprises 13 members of the National Council, the national parliament of Slovakia. This is an initiative and scrutiny body of the National Council in the field of national security and defence (including the organisation and activities of the armed forces), internal order and security, civil defence, state material reserves and the NSA. Concerning cyber security, the committee publishes a biannual Report on the state of use of ICT by the governmental security agencies with respect to the 166/2003 Act on Privacy Protection.[46] The committee has the right of legislative initiative and the right to 'invite to their sessions members of the Government, heads of central bodies of state administration other than ministries and the Prosecutor General and request from them reports, explanations and necessary documents.'[47]

The Ministry of Defence does not have a direct role in national cyber security management other than management of its own resources. However, due to the Ministry's role in identifying critical needs and developing requirements for national defence – in terms of composition of the forces and their capabilities – through the development of the *White Paper on Defence*, *Security Strategy of the Slovak Republic*, and the *Doctrine of the Armed Forces*, the Ministry also specifies the state's general cyber security needs. In the *White Paper on Defence*, the Ministry of Defence has recognised the challenges of cyber security and the need for military cooperation for defence against cyber attacks.[48]

Although intra-governmental and inter-departmental cooperation is recognised as a cyber security strategic priority, coordinated efforts among governmental agencies are not always assured. Nonetheless, little competition takes place and the autonomy of the Ministry of Finance and the NSA is largely respected, which is to attribute to the Committee for Information Security and open access points of most public administration agencies through which communication is managed.[49]

3.2. Cyber incident management and coordination

The national **Computer Security Incident Response Team of Slovakia**, CSIRT.SK, operates as an independent department of **DataCentrum**, an organisation financed from the budget of the Ministry of Finance.[50] The CSIRT is headed by a Director and has three subordinate departments: the Technical Department responsible for monitoring and gathering information about cyber security threats and risks; the National Information and Communication Infrastructure (NICI) Department which deals with incident handling; and an Education Department, which develops and implements education concepts for the security managers and ICT security staff of state and public institutions, and for the general public and cyber security professionals. The CSIRT

[45] The mentioned tasks are proposed by the director of NSO in the Working Programme of the Security Council of Slovak Republic for 2014, for spring 2014. Úradu vlády SR, Kancelária Bezpečnostnej rady SR, 'Plán práce. Bezpečnostnej rady Slovenskej republiky na rok 2014 (schválený uznesením vlády č.)', Bratislava, 2013 <http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-160793?prefixFile=m_>.

[46] Národná rada SR,'Správa. Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za I. polrok 2013', 605, 2013 <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=387866> (in Slovak), [*Report of the National Council for Defence and Security of the State of the Use Of Information and Technical Resources for The First Half Of 2013*].

[47] Established on the basis of Resolution of the National Council of the Slovak Republic No. 15. Národna rada SR, 'Postavenie a právomoci'<http://www.nrsr.sk/web/Default.aspx?sid=vybory/kompetencie>.

[48] White Paper on Defence (n 19) 29, 47-49, 51, 82, 85, 127.

[49] See: Information Security (n 38); National Strategy for Information Security (n 18) 13.

[50] DataCentrum is a budgetary organization created under the Ministry of Finance of the Slovak Republic. Computer Security Incident Response Team Slovakia (CSIRT.SK), 'CSIRT.SK Description Document According To RFC 2350' <https://www.csirt.gov.sk/csirtsk/rfc-2350-7e7.html>.

Information Specialist, directly subordinated to the Director, is the prime point of contact with regard to the customers and international cooperation.[51]

The Slovakian CSIRT provides a number of 'reactive services', including alerts and warnings based on analysis of security threats and vulnerabilities; manuals for addressing the most common incidents; analysis of incidents and malware; response to incidents and malware; and incident response coordination.[52]

Moreover, the CSIRT also engages in a set of proactive services, such as education, information distribution, awareness-building and consultancy in information security; threat monitoring in the field of ICT, infiltration detection, and information dissemination about threats and vulnerabilities; as well as configuration and infrastructure maintenance, and technology watch.[53]

The operation of the national CSIRT affects public institutions, commercial corporations, and a variety of organisations and individuals. In order for the CSIRT to effectively cover such a vast area of operation at varying levels of security, the competencies of the CSIRT must be clearly outlined. Currently, the legal framework outlining such competencies is in development.[54] Although the services of CSIRT are primarily aimed at the public administration, some services, such as published warnings, are freely accessible to a wide range of parties.

Most of the CSIRT.SK outreach to the private sector occurs through education activities.[55] Cooperation in the field of information security between the CSIRT.SK and the private sector is secondary to the team's focus on public administration, and the private sector is rarely involved in public-private partnerships due to a lack of opportunities on both sides.

Other Stakeholders

Although the CSIRT.SK is the only registered CSIRT in Slovakia, a number of organisations are dedicated to monitoring the state of security in their particular network. Among them are the **Sanet** (Slovak academic Network, member of TERENA), **ISACA Slovak Chapter**, **ITAS** (IT Association of Slovakia), **Sasib** (Slovak Association for Information Security).[56] Slovakia is also a part of the Central and Eastern European Networking Association (CEENet), whose primary mission is to 'co-ordinate the international aspects of the academic, research and education networks in Central and Eastern Europe and in adjacent countries', but their cooperation has evolved into computer network security.[57]

3.3. Military cyber defence

As noted above, the **Ministry of Defence** (MOD) includes cyber defence in its strategic vision (and strategic documents); however, cyber security is exercised for the most part as an organic capability exercised by the Ministry for its own needs. The MOD currently does not have the capacity, the ambition, or the potential to expand beyond its current remit. Within this structure, cyber security is orchestrated on two levels. One is

[51] Computer Security Incident Response Team Slovakia (CSIRT.SK), 'Vitajte!' <https://www.csirt.gov.sk/about-us/our-team-81f.html>.
[52] Computer Security Incident Response Team Slovakia (CSIRT.SK), 'Harmonogram vytvorenia CSIRT.SK' 4 <https://www.csirt.gov.sk/csirtsk/dokumenty-855.html>; Vitajte (n 51).
[53] ibid.
[54] Harmonogram vytvorenia CSIRT.SK (n 52) 1.
[55] See: Slovenská akademickej sieť (SANET), 'Organizačná štruktúra' <http://www.sanet.sk/organizacnastruktura.shtm>; ISACA Slovensko, 'IT Professional Networking and Knowledge Center', <http://www.isaca.sk/hlavne-menu/knowledge-center/>; IT Asociácie Slovenska (ITAS), 'Členovia ITAS' <http://itas.sk/clenovia>; Slovenská asociácia pre informačnú bezpečnos (SASIB) <http://www.sasib.sk/index.html>.
[56] ibid.
[57] European Union Agency for Network and Information Security (ENISA), 'CERT Cooperation and Its Further Facilitation by Relevant Stakeholders', Deliverable WP 2006/5.1(CERT-D3), 2006, 41 <http://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders>.

within the predominantly civilian MOD under the Department of CIS, Modernisation and Support Section, whose overarching role is to deliver technological and human resources as a support service for the Ministry. The second level falls within the **General Staff of the Armed Forces**, which addresses operational support through the Training and Support Forces, whose Division of Security and Protection of Information and CIS within the Department of Operational Support of the Training and Support Forces is the central provider of operational cyber security. The unit takes part in installing and maintaining the Ministry's information systems, while securing classified information, information systems, and managing cryptographic hardware and software in the course of its information assurance role.[58] It also shares the interoperability and partnership obligations of the Ministry and supports the development and compliance regarding norms concerning classified information, encryption standards, and the maintenance of CIS. The unit also maintains the registry of documents received from the EU and NATO.[59]

A change in the approach to cyber security came in 2013 when the MOD proposed its *Concept for Creating Capability for Monitoring, Evaluation and Measure-Taking in the Field of Information Security*.[60] The aim of this document was to create a **CSIRT.MIL.SK** in two-phases. The first (2013 to March 2014) would focus on the educational preparation of the expert personnel, and the second phase (April 2014 to March 2016) would involve the creation of a functional structure of cyber defence on all levels of the Ministry of Defence.

The monitoring, identification, and response to security incidents has until now been done only on *ad hoc* basis by the .mil domain administrators and the ZaSKIS expert groups. The CSIRT.MIL.SK, once set up, will become interoperable with foreign CSIRTs and counterparts in international organisations. Its responsibilities will expand to increasing the awareness of information security through educational schemes, maintaining a Computer Incident Response Capability, and providing defence against cyber attacks.

The team will be structured into the ZaSKIS (Base for Stationary Communication and Information Systems) in Trenčín, directly subordinated to the General Staff.[61] Among the major risks identified concerning the creation of the team is the lack of qualified personnel, which has been emphasised over financial and doctrinal issues. Personnel concerns remain in spite of the fact that the MOD has made an active effort to participate in cyber security internationally, *inter alia*, via its involvement in the NATO CCD COE in Tallinn. The team is intended to have a legal advisor as its disposal and is planned to include three functional groups: an analytical-technical group, a prevention and reaction group, and a group for research and special studies.

Although the team's remit has been clearly defined as restricted to covering the CIS of the MOD, some confusion about CSIRT.MIL.SK competencies has been awoken by the government's *Report on the Security of the Slovak Republic* for 2012. The report addresses repeated attacks by hacker groups targeting public administration institutions as well as other private sector institutions, which has increased the vulnerability of the whole of the information society. Therefore, the Report advocates a complex approach, integrating State defence with respect to cyber security. It is debatable whether the competency division among the MOD, Ministry of Finance and the NSA complements this complex approach. On the other hand, the White Paper highlights the importance of securing the information systems of the Armed Forces from a cyber attack before a multi-sector security can be achieved.[62]

3.4. Intelligence

The **Slovak Information Service** is the 'central intelligence and security service of the Slovak Republic that guarantees intelligence protection of the country.'[63] It is tasked to collect among other things technical

[58] Veliteľstvo síl výcviku a podpory os SR, 'Odbor pre podporu operácií' <http://www.vsvap.mil.sk/6800/>.
[59] Veliteľstvo síl výcviku a podpory os SR, 'Oddelenie BOI a KIS' <http://www.vsvap.mil.sk/6806/>.
[60] Approved on the basis of Working Plans of the Army Council for 2012 No. KaNGŠ/P-2/2013/2013.
[61] Correspondence with the Chief of BOIaKIS - J6, ŠbPO GŠ OS SR.
[62] Report 2012 (n 19) 4 para 7; See also: White Paper on Defence (n 19) 64 § 244.
[63] The Slovak Information Service (SIS) 'About SIS' <http://www.sis.gov.sk/about-us/about-sis.html>.

intelligence and Open Source Intelligence (OSINT) and to share it with other law-enforcement bodies as well as particular EU platforms and NATO structures.[64] The agency is overseen by the Government and the Security Council in particular.[65]

3.5. Cyber aspects of crisis management

All critical information infrastructure, including the information systems of a particular sector of critical infrastructure, is subject to the *Act No. 45/2011 on Critical Infrastructure*.[66] The responsibility for coordinating the implementation of the Act is allocated to the Ministry of Interior together with other Ministries with sectoral and sub-sectoral responsibility. The ministries represent a conduit between privately owned national critical infrastructure and European critical infrastructure, and are obligated to keep a non-public central register of all critical infrastructure elements.

SECTOR	SUBSECTOR	ORGANISATION
ICT	Information Systems and Networks, Internet	Ministry of Finance, CSIRT.SK
Electronic Communications	Satellite communication, networks and stable and mobile services of electronic communications	Ministry of Transport, Construction and Regional Development
Transport	Road, air, water, rail	Ministry of Transport, Construction and Regional Development
Post	Post services, system of payments and procurement activities	Ministry of Transport, Construction and Regional Development
Health		Ministry of Health
Energy	Electricity, Gas, crude Oil, Mining	Ministry of Economy
Water and Atmosphere	Drinking water, water construction, meteorology	Ministry of Economy
Industry	Pharmaceutical, chemical, metallurgical	ME Slovak Republic

The specificity of the information systems as a part of critical infrastructure and their identification and classification should be a part of the forthcoming *Act on Information Security*.[67]

It is the responsibility of the information security coordinator or owner of the infrastructure to implement a Security Plan and to modernise the technology used for securing a critical infrastructure element. The Security Plan lists the potential threats of disruption or damage to the referent critical infrastructure element and the security measures to be taken for its protection; the Plan is overseen by the agency of public administration central to the sector and the Government.[68] For governmental information systems, security standards are defined in *Decree No. 312/2010 Coll*.

Slovakia has participated in critical infrastructure protection exercises, namely Cyber Europe 2010, Cyber Atlantic EU-US 2011, and the SISE 2011 and 2012.[69]

---

[64] The Slovak Information Service (SIS) 'SIS Tasks' <http://www.sis.gov.sk/about-us/sis-tasks.html>.
[65] The Slovak Information Service (SIS) 'Oversight' <http://www.sis.gov.sk/about-us/coordination-and-oversight.html>.
[66] Zákon o kritickej infraštruktúre (n 33) , § 2 (a).
[67] Informatizacia.sk, 'Návrh. Legislatívny zámer zákona o informačnej bezpečnosti. Úvod', 1, 10 <http://www.informatizacia.sk/ext_dok-zamer_zakona_o_ib/9131c>.
[68] Zákon o kritickej infraštruktúre (n 66) § 5 (l) (6), § 6 (f), § 9 (1), § 10. The measures include mechanic and technical means, information security systems, physical protection, and organisational and control measures.
[69] Ján Hochmann *et al*, 'Aims Fulfilment of the National Strategy for Information Security of the Slovak Republic', 6th STAR Workshop on Digital Security, 2012 <http://www.scholze-simmel.at/starbus/ws6/wp-content/uploads/Hochmann.pdf>. The chain of responsibility in MF SR goes back to Information Society Section, Department of information Technologies, Internal Information Security Division; the MTCRD SR delegates its Department of Electronic Communications and the Interior. See also: Computer Security Incident Response Team Slovakia (CSIRT.SK), DataCentrum, 'Brochure' <https://www.csirt.gov.sk/img/infobrochure-eng.pdf>.

The Act on Critical Infrastructure does not deal with crisis management, which is subject to Act 319/2002 on Defence of Slovak Republic and Act No. 110/2004 on the Functioning of the Security Council of Slovak Republic in Peacetime.[70] Constitutional Act No. 227/2002 Coll. on State Security at the Time of War, State of War, State of Emergency, and State of Crisis defines a crisis situation as a time period during which is the security of the state imminently threatened or breached.[71] This legislation provides general guidance on crisis management, but without a particular focus paid to cyber crisis.

In practice, the pervasiveness of security incidents has meant that measures are determined by organisational culture rather than by existing legislation. Some incidents are addressed on an *ad hoc* basis only once the functioning of ICT systems is threatened, while others are handled as they arise in an effort to keep pace with the development of potential threats. In this respect, the data on the numbers of incidents experienced in organisations is unreliable, but in general a rising trend in report submission can be observed.[72]

[70] See: Ministerstvo obrany SR, 'Zákony v pôsobnosti Ministerstva obrany Slovenskej republiky' <http://www.mosr.sk/zakony-v-posobnosti-ministerstva-obrany-slovenskej-republiky/>.
[71] Zákony pre ľudí.sk, 'Ústavný zákon o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu', Predpis č. 227, 2002, § 1 (4), § 8 (2), § 9 <http://www.zakonypreludi.sk/zz/2002-227>.
[72] Ján Hochmann *et al*, 'Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike v roku 2013', Ministerstvo financií SR, 2013, 15-16 <http://www.informatizacia.sk/ext_dok-prieskum_ib_2013_-sk-en-/16943c>.

References

Computer Security Incident Response Team Slovakia (CSIRT.SK), 'CSIRT.SK Description Document According To RFC 2350' <https://www.csirt.gov.sk/csirtsk/rfc-2350-7e7.html>.

Computer Security Incident Response Team Slovakia (CSIRT.SK), DataCentrum, 'Brochure' <https://www.csirt.gov.sk/img/infobrochure-eng.pdf>.

Computer Security Incident Response Team Slovakia (CSIRT.SK), 'Harmonogram vytvorenia CSIRT.SK' <https://www.csirt.gov.sk/csirtsk/dokumenty-855.html>

Computer Security Incident Response Team Slovakia (CSIRT.SK), 'Vitajte!' <https://www.csirt.gov.sk/about-us/our-team-81f.html>.

Council of Europe, 'Convention on Cybercrime', CETS No. 185, Budapest, 2001 <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

EU Digital Agenda, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard' <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"egovernment","ref-area":"SK","time-period":"2013"}>.

European Commission, 'Country Information - Slovak Republic', 2014 <http://ec.europa.eu/digital-agenda/en/country-information-slovak-republic>.

European Commission, eGovernment Factsheets, 'eGovernment in Slovakia', Edition 16.0, 2014 <https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGov%20SK%20-%20April%2014-v_16_0.pdf>.

European Union Agency for Network and Information Security (ENISA), 'CERT Cooperation and Its Further Facilitation by Relevant Stakeholders', Deliverable WP 2006/5.1(CERT-D3), 2006 <http://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders>.

Eurostat <http://ec.europa.eu/eurostat/help/new-eurostat-website>.

ISACA Slovensko, 'IT Professional Networking and Knowledge Center', <http://www.isaca.sk/hlavne-menu/knowledge-center/>.

Ján Hochmann et al. 'Aims Fulfilment of the National Strategy for Information Security of the Slovak Republic', 6th STAR Workshop on Digital Security, 2012 <http://www.scholze-simmel.at/starbus/ws6/wp-content/uploads/Hochmann.pdf>.

Hochmann, Ján et al, 'Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike v roku 2013', Ministerstvo financií SR, 2013 <http://www.informatizacia.sk/ext_dok-prieskum_ib_2013_-sk-en-/16943c>.

Informatizacia.sk, 'Návrh. Legislatívny zámer zákona o informačnej bezpečnosti. Úvod', 1, 10 <http://www.informatizacia.sk/ext_dok-zamer_zakona_o_ib/9131c>.

IT Asociácie Slovenska (ITAS), 'Členovia ITAS' <http://itas.sk/clenovia>.

Ministerstvo financií SR, 'Kontakty' <http://informatizacia.sk/kontakty/4795s>.

Ministerstvo financií SR, 'Národná stratégia pre informačnú bezpečnosť v Slovenskej republike', 2008 <http://www.informatizacia.sk/ext_dok-narodna_strategia_pre_ib/6167c>.

Ministerstvo financií SR 'Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike v roku 2013' 2013, 5 <http://www.informatizacia.sk/prieskum-stavu-ib/12772s>.

Ministerstvo obrany SR, 'Zákony v pôsobnosti Ministerstva obrany Slovenskej republiky'

<http://www.mosr.sk/zakony-v-posobnosti-ministerstva-obrany-slovenskej-republiky/>.

Ministerstvo vnúra SR, 'Nenájdený dokument' <http://www.minv.sk/?sekcia_izs_km_mvsr>.

Národna rada SR, 'Postavenie a právomoci'<http://www.nrsr.sk/web/Default.aspx?sid=vybory/kompetencie>.

Národná rada SR,'Správa. Výboru Národnej rady Slovenskej republiky pre obranu a bezpečnosť o stave použitia informačno-technických prostriedkov za I. polrok 2013', 605, 2013 <http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=387866>.

Národný bezpečnostný úrad (NBÚ), 'Štruktúra úradu' <http://www.nbusr.sk/sk/struktura-uradu.1.html>.

National Security Authority (NBÚ), 'National Security Authority' <http://www.nbusr.sk/en/>.

Office of the Government of the Slovak Republic, 'Operational Programme Informatisation of Society', Version 4.0, Bratislava, 2012 <http://www.opis.gov.sk/data/files/2448_8949.pdf>.

Office of the Government of the Slovak Republic, 'Statute of Security Council of Slovak Republic', Resolution No. 162, 28 February 2007, Art. 1-2, 6, 8 <http://www.government.gov.sk/statute-of-the-government-office-of-the-slovak-republic/?pg=2>.

'Opatrenie - Akčný plán informačnej bezpečnosti' <http://www.informatizacia.sk/ext_dok-akcny_plan_k_strategii_pre_ib/6790c>.

Sekcia informatizácie spoločnosti, 'Členenie a Pôsobnosť odborov/oddelení Sekcie informatizácie spoločnosti', 2008 <http://www.informatizacia.sk/sekcia-informatizacie-spolocnosti/5188s>.

'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2009 <http://www.informatizacia.sk/ext_dok-sprava_2009_strategia_a_akcny_plan_ib/6788c>.

'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2011 <http://www.informatizacia.sk/ext_dok-sprava_2011_strategia_a_akcny_plan_ib/16198c>.

'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2012 <http://www.informatizacia.sk/ext_dok-sprava_2012_strategia_a_akcny_plan_ib/16200c>.

'Správa o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR', 2013 <http://www.informatizacia.sk/ext_dok-sprava_2013_strategia_a_akcny_plan_ib/16201c>.

Slovenská akademickej sieť (SANET), 'Organizačná štruktúra' <http://www.sanet.sk/organizacnastruktura.shtm>; <http://www.isaca.sk/hlavne-menu/knowledge-center/>.

Slovenská asociácia pre informačnú bezpečnos (SASIB) <http://www.sasib.sk/index.html>.

Slovenskej republiky, 'Zákon o kritickej infraštruktúre', Zbierka zákonov č. 45, 2011 <www.zbierka.sk/sk/predpisy/45-2011-z-z.p-33998.pdf>.

Zákony pre ľudí.sk, 'Ústavný zákon o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu', Predpis č. 227, 2002 <http://www.zakonypreludi.sk/zz/2002-227>.

The Boston Consulting Group (BCG), 'Slovakia Online - How the Internet Is Transforming the Slovak Economy', 2012 <http://www.onlinesanca.sk/pdf/BCG_Google%20Slovakia%20Online_EN.pdf>.

The Ministry of Defence of the Slovak Republic, 'The White Paper on Defence of the Slovak Republic', 2013 <http://www.mosr.sk/data/WP2013.pdf>.

The Ministry of Finance of the Slovak Republic, 'Information Security' <http://informatizacia.sk/information-security/4622s>.

The Ministry of Finance of the Slovak Republic, 'Information Society Strategy for 2009–2013', Bratislava, 2009 <http://www.informatizacia.sk/ext_dok-information-society-startegy-for-2009_2013/6497c>.

The Ministry of Finance of the Slovak Republic, 'National Strategy for Information Security in the Slovak Republic (NSIS)', 2008 <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf>

The Slovak Information Service (SIS) <http://www.sis.gov.sk/index_en.html>.

Úradu vlády SR, Kancelária Bezpečnostnej rady SR, 'Plán práce. Bezpečnostnej rady Slovenskej republiky na rok 2014 (schválený uznesením vlády č.)', Bratislava, 2013 <http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-160793?prefixFile=m_>.

Úradu vlády SR 'Spoločný rokovací poriadok Bezpečnostnej rady kraja', 26. februára 2003, Čl. 3, 4 <http://www.vlada.gov.sk/spolocny-rokovaci-poriadok/>.

Veliteľstvo síl výcviku a podpory os SR <http://www.vsvap.mil.sk/1309/home.php>.