CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Vytautas Butrimas

National Cyber Security Organisation: LITHUANIA

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 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 Hungary

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 September 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.

LITHUANIA

By Vytautas Butrimas
Adviser, Lithuanian Ministry of National Defence;
Member, Lithuanian National Communications Regulatory Authority Council

Table of Contents

1. INTRODUCTION: INFORMATION SOCIETY INDICATORS 5

1.1. INTERNET INFRASTRUCTURE AVAILABILITY AND TAKE-UP 5

1.2. AVAILABILITY AND USE OF E-SERVICES 6

1.2.1. Public sector e-services: e-government 6

1.2.2. Private sector e-services: e-commerce and e-business 6

2. STRATEGIC NATIONAL CYBER SECURITY OBJECTIVES 7

2.1. NATIONAL CYBER SECURITY FOUNDATION 7

2.2. NATIONAL CYBER SECURITY OBJECTIVES AND PRIORITIES 8

2.3. NATIONAL CYBER SECURITY LEGISLATION 8

3. CYBER SECURITY ORGANISATIONAL STRUCTURE 9

3.1. CYBER SECURITY POLICY COORDINATION 9

3.2. CYBER INCIDENT MANAGEMENT AND COORDINATION/OPERATIONAL CYBER SECURITY 10

3.3. MILITARY CYBER DEFENCE 11

3.4. CYBER CRISIS MANAGEMENT 11

3.5. CYBER INTELLIGENCE 12

3.6. PRIVATE SECTOR INVOLVEMENT 12

CLOSING REMARKS 13

REFERENCES 14

1. Introduction: information society indicators

Lithuania is building its cyber security capacity and management institutions based on a long tradition in information technology and telecommunications. Before the breakup of the Soviet Union, Lithuania had established an IT industry that included the design and manufacture of IT hardware and software. A successful partnership was developed between government, industry, and education establishments to support this industry. At the end of the 1980s the Sigma manufacturing group consisted of seven plants employing over 18,000 people in production and management, and 2000 in research and development. Production of computers ranged from cloned versions of DEC VAX 730 mainframes to the first IBM clone personal computers.[1] However, this unique IT industrial base faded away soon after the re-establishment of Lithuania's independence in 1990, due to the subsequent halt in Soviet contracts and because of insufficient investment capital for modernisation to western manufacturing standards. The new independent Government of the Republic of Lithuania soon took its first steps toward creation of an information society by creating the Ministry of Communications and Informatics (MCI). In 1993 the Government approved MCI's State Communications and Informatics development program for the modernisation of the state's communications and information infrastructure including provisions for developing appropriate legal acts and standards needed for establishing the basic elements of information infrastructure.[2]

1.1. Internet infrastructure availability and take-up

Lithuania has developed a broadband-based internet infrastructure available to its citizens. In 2014 it had a broadband infrastructure consisting of 23,700 km of fibre cables, with about 11,700 km owned by private communication companies.[3] This fibre optic network infrastructure has 27 international connections with neighbouring countries Poland, Sweden, Latvia, Russia and Belarus.[4] In terms of number of internet users and broadband internet penetration, Lithuania has done well. At the end of 2014 Lithuania had over 1,200,000 internet subscribers out of population of 3 million. The broadband penetration rate, including those who connected using fixed and mobile technologies, was 43%.[5] Many also make use of mobile internet services to access the internet in Lithuania. The number of subscribers who used public mobile data services (internet access) provided by 3G and 4G mobile communication networks via computer and smart phone at the end of 2014 was over 1,7000,000 or 60.3%. Most of these users used their mobile telephones as means of access to the internet.[6]

In addition to extending internet infrastructure to major cities and towns in Lithuania, rural areas have also been included. The project to provide broadband internet services to rural areas (RAIN) attempts to address the imbalance in the availability of broadband between cities and rural areas which was 99% and 32% percent respectively.[7] The second phase is nearing completion and will have done much to equalise availability of broadband. At the end of 2015 a total of 4,915 km of fibre optic cable will have been laid and over 775 rural points[8] connected with internet connectivity provided by 48 service providers.[9]

[1] L. Telksnys, A. Žilinskas, 'Computers in Lithuania', IEEE Annals of the History of Computing, Vol. 21, No. 3, 1999 http://www.mii.lt/files/telk_zil_annals.pdf.

[2] Istorija' (History) http://www.ivpk.lt/lthm/istorija.

[3] Ministry of Transport contracted report prepared by closed stock company UAB 'InComSystems', Plačiajuosčio ryšio infrastruktūros plėtros ir paslaugų naudojimo skatinimo modelio parengimo paslaugų galutinė ataskaita, 2014 (Report on a model for stimulating the development and use of communications infrastructure and services), http://www.ivpk.lt/uploads/Leidiniai/Galutinė%20ataskaita.pdf, 27.

[4] ibid, 28.

[5] Lithuanian National Communications Regulatory Report on the electronic communications sector Quarter IV, 2014, 30. http://www.rrt.lt/en/reviews-and-reports/reports-on-the-urpp/2014_1098.html Updated on 2015-04-24.

[6] ibid, 34.

[7] Projekto prielaidos (Project assumptions) http://placiajuostis.lt/lt/projekto-prielaidos2.

[8] Šviesolaidinė infrastruktūra (fiber optic infrastrcuture) http://placiajuostis.lt/lt/sviesolaidine-infrastruktura2.

[9] ibid., http://placiajuostis.lt.

1.2. Availability and use of e-services

1.2.1. Public sector e-services: e-government

The people of Lithuania are offered access to a variety of e-Government services. The web portal https://www.epaslaugos.lt/portal/ offers a wide range of popular e-services to citizens and business ranging from declaring one's official place of residence to getting a certificate for the distribution of seeds for planting.[10] Many fill out and submit their yearly earnings declaration using the Electronic Declaration Service provided by the State Tax Inspectorate[11] (STI).[12] Users each year access their account on-line where their declaration has data provided to the STI by the employer already filled in.

Perhaps the most comprehensive in terms of potential impact on citizen's lives is the introduction of a centralised e-Health system in June of 2015. 'E-sveikata' (e-Health) when fully implemented will consist of a centralised information system and electronic prescription and medical images, together with the information systems of connected healthcare institutions throughout Lithuania.[13] People will be able to access their histories, view test results, prescription information, a vaccination calendar, appointment notices, order medical certificates, and make appointment with a doctor. It is intended that the principle of one inhabitant – one electronic patient history will be implemented in this new service.[14] The first services of this new system are to be made available to the public by the end of this year as healthcare institutions are connected to the system according to an order from the Minister of Health. Full implementation is planned to take place by the end of the first quarter of 2018.[15]

In the area of e-government, however, the majority of inhabitants do not take advantage of e-Government services. Only 41% (below the EU average) of Lithuania's citizens make use of available e-Government services and 31% (above the EU average) use them to complete and submit electronic forms to provided e-Government services.[16] Perhaps this statistic will change in a more positive direction after the e-Health system and other services are fully implemented.

1.2.2. Private sector e-services: e-commerce and e-business

Lithuania has established the necessary mix of infrastructure, laws, and services for e-commerce. Use of electronic signatures was approved by law in 2000[17] and appropriate infrastructures required for its implementation are in place. Currently three certificate authorities in Lithuania provide certificate services. Certificates for electronic signature use are employed using the inhabitant ID card, state employee cards, USB tokens or through the use of a SIM card provided by the mobile phone operator. By the end of 2014 there were nearly 900,000 qualified certificates in Lithuania.[18] While 36 percent of inhabitants of 18 years of age and over

[10] Populiariausios paslaugos (List of most popular e-services) https://www.epaslaugos.lt/portal/.

[11] Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos.

[12] Elektroninio deklaravimo sistema (Electronic declaration system), http://deklaravimas.vmi.lt/lt/Pradinis_Prisijungimo_puslapis/Prisijungimasperisorinessistemas.aspx.

[13] Lietuvos e sveikatos sistema pradeda veikti (Lithuania's e health system starts operating) http://www.15min.lt/naujiena/aktualu/sveikata/lietuvos-e-sveikatos-sistema-pradeda-veikti-541-507348 Published: 2015 June 3.

[14] ibid.

[15] Dėl elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudojimo tvarkos aprašo patvirtinimo (Minister of Health order of 2015 May 26 On the use of the E-Health Services and cooperation infrastructure information system) 2015 m. gegužės 26 d https://www.e-tar.lt/portal/lt/legalAct/f984390005c011e588da8908dfa91cac.

[16] Country (Lithuania) profiles, the relative position against all other European countries. http://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={"indicator-group":"egovernment","ref-area":"LT","time-period":"2014"}.

[17] Lietuvos Respublikos elektroninio parašo įstatymas (Republic of Lithuania Law on electronic signatures) https://www.e-tar.lt/portal/lt/legalAct/TAR.382345294FBF/TAIS_463802.

[18] Ryšių reguliavimo tarnybos 2015-03-31 LR Electroninio parašo įstatymo įgyvendinimo 2014 metų ataskaita (Communication regulatory annual report on implementation of Law on Electronic Signature 2015-03-31), http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroninio-paraso-istatymo-1b73.html.

have cards with valid certificates, many are unaware that their cards have this function.[19] Businesses in Lithuania have come to see the usefulness of using electronic signatures. In 2014, 87% of manufacturing and services enterprises consisting of 10 or more workers used electronic signatures.[20] In addition, Lithuania's banks have adapted their e-banking systems to accept electronic signatures and the popularity of this is increasing – one bank chain in Lithuania reported over 177,000 e-signed bank transactions over a 3 month period in 2014.[21]

Many in Lithuania, especially city dwellers, have become used to paying their monthly utility bills and making other payments electronically using the e-banking services. In 2014, according to a bank of Lithuania survey, 56% of those surveyed indicated that they pay for these services over the internet rather than in cash.[22] Overall payment habits for everyday transactions are changing. Of those surveyed 22% used a debit or credit card for payment in 2014.[23] In terms of individual citizen participation in e-commerce, however, Lithuania ranks below the EU average while Lithuania's business enterprise use of e-commerce for buying and selling is higher than the EU average.[24]

2. Strategic national cyber security objectives

Lithuania's efforts to achieve its national cyber security objectives have been characterised by both top-down and bottom-up approaches. Bottom-up efforts refer to establishing cyber security institutions without a single comprehensive law that clearly defines the responsibilities and field of activity in relation to other related cyber security institutions. Top-down refers to passing a comprehensive law that clarifies the role of previously created institutions or creates new cyber security institutions in a framework of defined institutional hierarchy (designating a national coordinator), assigning responsibility and a scope of activity to each entity. Examples of bottom-up efforts are the establishment of the Personal Data Inspectorate in 1999, Government authorising the National Communications Regulatory Authority to establish a National Computer Emergency Response Team (CERT-LT[25]) in 2006, and Government approval in 2011 of a programme for the development of electronic information security (cyber security) for 2011-2019.[26] The current pre-eminent model in Lithuania is top-down, as expressed in the 2014 Law on Cyber security which will be later discussed in more detail.

2.1. National cyber security foundation

First, as background to the Cyber Security Law, reference must be made to the Government-mandated inter-institutional task force on cyber security chaired by the Ministry of National Defence, which submitted its report of cyber Security recommendations to the Government in 2008.[27] Among the recommendations of the report which later received Government approval were: preparation of a National Cyber Security Strategy and delaying a decision on designating an institution to develop and coordinate national cyber security policy to

[19] ibid.

[20] ibid.

[21] ibid.

[22] Lietuvos gyventojų mokėjimo įpročių apklausos apžvalga 2014 (Lithuanian inhabitants' payment habits survey 2014) Bank of Lithuania ISSN-2335-81302, http://www.lb.lt/lietuvos_gyventoju_mokejimo_iprociu_apklausos_apzvalga_1.

[23] ibid.

[24] Digital agenda for Europe, Country profiles, the relative position against all other European countries, eCommerce indicators (Lithuania) 2014 http://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={"indicator-group":"ecommerce","ref-area":"LT","time-period":"2014"}.

[25] About CERT-LT, https://www.cert.lt/en/index.html.

[26] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą (The Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019), http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=403385.

[27] Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita (Prime Minister's 2008-06-17 tasking Nr. 225 Workgroup report on recommended course and measures for strengthening cyber security in Lithuania).

coincide with passage of a law on the security of electronic networks and information.[28] For various reasons, no National Cyber Security Strategy has been approved in Lithuania. To go back to the legal foundation for Lithuania's national cyber security, there is the Law on the Fundamentals of National Security passed in 1996. The law lists the national economic sectors which are significant to national security – energy, transport, information technology and telecommunications, other high-technology, finance and credit.[29] The Seimas (Parliament) of Lithuania later approved the National Security Strategy, which declared cyber security to be one of the priority national interests.[30] Among national security threats are listed cyber-attacks which threaten information and communications systems used in the economic sector, operation of vital state institutions, security of classified information, and other targets which threaten other vital functions of the state and well-being of citizens.[31]

2.2. National cyber security objectives and priorities

According to the 29 June 2011 Government Resolution Nr. 766 On the approval of The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019 there are 3 main program objectives: (1) To insure the security of state-owned information resources; (2) To insure an efficient functioning of critical information infrastructure; (3) To seek to ensure the cyber security of the Lithuanian residents and persons staying in Lithuania.[32] These objectives have been carried over and further developed in the Law on Cyber Security approved in 2014.

2.3. National cyber security legislation

The cyber security organisational structure of Lithuania is defined today by the Law on Cyber Security passed on 11 December 2014. The significant points include the transfer of the national cyber security policy coordination function to the Ministry of National Defence (MoND), establishment of a new operational National Cyber Security Centre (NCC)[33] under the MoND, creation of an Advisory Council on Cyber Security chaired by the MoND, and establishment of a cyber security stakeholder information sharing network (CISN) managed by NCC. The Ministry of Interior and its cyber-crime unit (CCU), Personal Data Inspectorate, and the Communication Regulatory Authority (National CERT) which existed before the law were included in the new national cyber security organisational structure and assigned responsibilities as defined in the law. Also significant is the inclusion and attention given to the cyber security of Hosting Services[34] (HS), Critical

[28] LR Vyriausybes pasitarimo protokolas 2009 m. balandžio 15 d. Nr. 29 18. Dėl LR Ministro Pirmininko 2008 m. birželio 17 d. potvarkio Nr. 225 sudarytos darbo grupės Lietuvos kibernetinio saugumo klausimams išnagrinėti ir pasiūlymams dėl jo stiprinimo parengti pasiūlymo įgyvendinimo (Government meeting protocol of 2009 April 15 Nr. 29 agenda item 18 Regarding Prime Minister's 2008-06-17 tasking Nr. 225 on Workgroup report on recommended course and measures for strengthening cyber security in Lithuania).

[29]Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas 1996 m. gruodžio 19 d. Nr. VIII-49 (Law on fundamentals of national security) http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=442449.

[30] Lietuvos Respublikos Seimas nutarimas dėl nacionalinio saugumo strategijos patvirtinimo 2002 m. gegužės 28 d. Nr. IX-907, III. 8.8 (Seimas of the Republic of Lithuania 2002 May 28 decree nr. IX-907 on National Security Strategy) http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=429234.

[31] ibid. IV. 10.5. kibernetinės atakos – elektroninių ryšių tinklų ir informacinių sistemų atakos, kuriomis siekiama sutrikdyti nacionaliniam saugumui strategiškai svarbių ūkio sektorių infrastruktūros funkcionavimą ir nacionaliniam saugumui svarbių valstybės institucijų veiklą, išgauti įslaptintą informaciją, vykdyti kitas nusikalstamas veikas ir taip pakenkti valstybės ir jos piliečių saugumui.

[32] Government 29 June 2011 Resolution Nr. 796. II-(6.1 – 6.3) Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą (The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019) http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=403385.

[33] Nacionalinis kibernetinio saugumo centras (National cyber security centre) web page. http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/rysiu_ir_informaciniu_sistemu_tarnyba_prie_kam_2482/nacionalinis_kibernetinio_saugumo_centras.html.

[34] Hosting Services, http://www.webopedia.com/TERM/H/hosting_services.html.

Information Infrastructure (CII) and Industrial Control Systems (ICS) in the text of the law.[35] CII is defined as an electronic communications network or part of it, an information system or part of it, a group of information systems or industrial control system or part of it, regardless of whether the administrative owner is from the public or private sector, where a cyber-incident can cause harm to national security, economy, state or public interest.[36] Industrial control systems are defined in the law as information and communications technology based equipment forming a system, designed to monitor and manage technological processes found in sectors of manufacturing, energy, transport, water supply services and other sectors of economic activity.[37] The addition of ICS is in part explained by the realisation that information and communications systems that are so closely associated with the information society and all modern services are dependent upon the reliability and availability of services provided by critical infrastructure; for example information technology and communications need electricity from power grids to function.

The relationship and functions of the institutions as defined in the Law on Cyber Security are depicted in Figure 1.

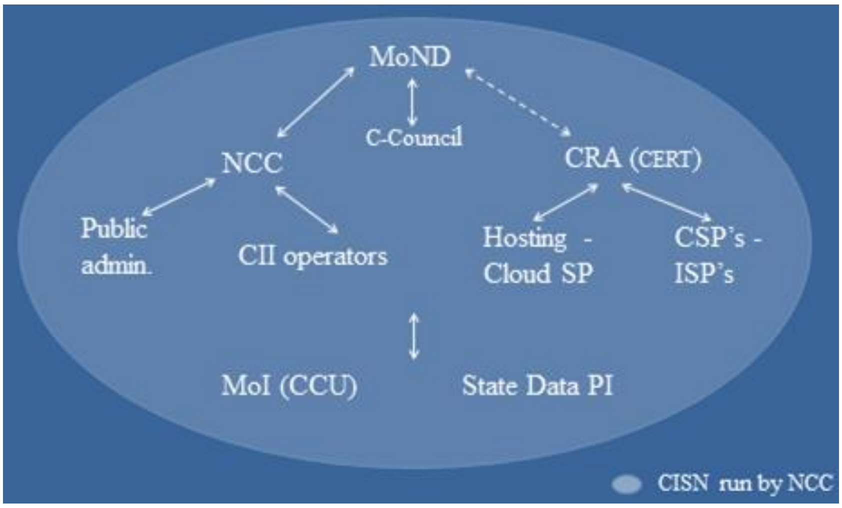

Figure 1. Cyberspace security management structure according to the Law on Cyber Security

3. Cyber Security Organisational Structure

3.1. Cyber security policy coordination

As outlined in the law on Cyber Security, the Ministry of National Defence has the responsibility to formulate and coordinate implementation of cyber security policy in Lithuania. This new function has been realised in the MoND by the creation of a new department dedicated to cyber security and information technology.

The newly created Cyber Security Council (C-Council) is a national level advisory group on cyber security policy chaired by the MoND and includes representatives from the public, private, and academic sectors.[38] The main functions of the C-Council are: (1) to prepare and submit proposals to the cyber security Community of Interest

[35] Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (Cyber security law of the Republic of Lithuania 11 December 2014 Nr. XII-1428, I-2. https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.

[36] ibid. I-2.2. Ypatingos svarbos informacinė infrastruktūra (Critical information infrastructure) – unofficial translation from Lithuanian text).

[37] ibid. I-2.6. Pramoninių procesų valdymo sistema (Industrial control system) – unofficial translation.

[38] LRV 2015 m. balandžio 23 d. Nutarimas Nr. 422 Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo (Government decree on approval of the cyber security council and regulation) https://www.e-tar.lt/portal/lt/legalAct/4e3539f0ee4611e4927fda1d051299fb.

(CoI)[39] regarding priorities, areas of focus for further activity, propose goals and means to achieve them; (2) to prepare and submit proposals to the CoI for wider public, private and research cooperation in the area of cyber security; (3) to analyse cyber security implementation methods and provide the CoI proposals for more effective management of cyber incidents; and (4) to submit the CoI with recommendations for strengthening cyber security.[40]

3.2. Cyber incident management and coordination/operational cyber security

Under the MoND the National Cyber Security Centre (NCC)[41] is in direct contact with the public sector and with the operators of critical information infrastructure. The NCC manages the cyber security information sharing network which is used to exchange cyber security related information among the community of interest (CoI). The NCC also maintains a system of sensors to monitor cyberspace with a focus on protection of critical information infrastructure. According to the law each institution is responsible for appointing a cyber security officer or creation of a cyber security unit which also acts as a point of contact for liaison with the NCC. Cyber security incidents occurring in the institution are required to be reported to the NCC. The NCC has the legal right to instruct managers of public sector institutions and CII operators within its authority in responding to a reported cyber incident.[42]

The Ministry of Interior is responsible for the preparation of the CII identification methodology and for presenting the list of CII to the Government for approval. At the time of writing the list had yet to be approved, but there is an officially approved list of critical objects and equipment in the Law on Enterprises and Equipment of Strategic Importance to National Security originally passed in 2002.[43] However, cyber threats to CII are not specifically mentioned in this law.[44] This is a key factor in the implementation of the Law on Cyber Security as it will not fully be implemented until the MoI submits for approval the official CII list. The approval of the list will clarify which institutions fall under compliance with the law such as the requirement for reporting of incidents and meeting the security policies mandated.[45]

The Communications Regulatory Authority (CRA)[46] already has responsibilities mandated according to the Law on Communications[47] for regulating the communications sector and operates a National CERT as previously authorised by the Government. According to the new cyber security law the CRA's CERT now has a direct

[39] In addition to the MoND which chairs the Council also represented are: 'IT association Infobalt ', Kaunas University of Technology, Vilnius University, Closed stock company 'Lithuania Energy', Heating association of Lithuania, Water supply association of Lithuania, Bank of Lithuania, Bank Association of Lithuania, Criminal Police Bureau, State Data Protection Inspectorate, Government Ministries(Energy, Transportation, Justice, Interior, Foreign affairs, Economy), Communications Regulatory Authority, and State Chancellery.

[40] Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (Cyber security law of the Republic of Lithuania 11 December 2014 Nr. XII-1428, II-9-4(1-4). https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.

[41] Lithuanian: Nacionalinis kibernetinio saugumo centras.

[42] Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (Cyber security law of the Republic of Lithuania 11 December 2014 Nr. XII-1428, II-10.11-4. https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.

[43] Strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas (Law on enterprises and equipment of strategic importance to national security) 2002 October 10 Nr. IX-1132.

[44] Physical and information security requirements (fizinės ir informacinės saugos reikalavimus) are mentioned but it is not clear whether cyber aspects are specifically included. ibid., 9 (1-2).

[45] As of the time of the writing of the article (summer of 2015) there is only an interim, unapproved, list of CIP which is being used until the official list is approved by the Government.

[46] Lietuvos Respublikos ryšių reguliavimo tarnyba.

[47] Lietuvos Respublikos elektroninių ryšių įstatymas (Law on electronic communications) 2004 april 15 Nr. IX-2135 (II-(6-9)) http://www3.lrs.lt/pls/inter3/oldsearch.preps2?Condition1=232036&Condition2=

relationship with hosting services, communications and internet service providers. It has the legal right to instruct service providers within its authority in responding to a reported cyber incident.[48]

In cases of reported cyber incidents involving cybercrime, the MoI Cyber Crime Unit (CCU)[49] will be called upon to investigate.[50] It has the legal right during an investigation of cybercrime to give appropriate instructions to service providers.[51]

Cyber security incidents involving the misuse of personal data are evaluated and acted upon by the State Data Protection Inspectorate (SDPI)[52] which supervises and monitors the implementation of the law on the legal protection of personal data.[53]

3.3. Military cyber defence

In December of 2009 the Minister of National Defence approved the first National Defence System Cyber security Strategy and Implementation Plan, which was updated and approved again in 2013.[54] The strategy emphasises insuring the secure transfer of electronic information, the cyber security of National defence system institutions and to contribute to protecting the cyber security of the state's critical information infrastructure.[55] The MoND established its CERT in 2009, and today it operates under the Cyber security and Telecommunications Service (CTS)[56] under the MoND. The CERT was initially created to monitor and respond to cyber incidents on national defence system data transfer networks, but the Ministry later signed memorandums of understanding for cooperation in cyber security with the Communications Regulatory Authority and Ministry of Foreign Affairs. After the passage of the Cyber security Law the MoND-CERT under the CTS was expanded to also include the core functions of the National Cyber security Centre.

Since 2009 the MoND has a cooperative relationship that included meetings and consultations with cyber security institutions in Latvia and Estonia. Lithuania is one of the founding nations of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia.

The MoND also cooperates as a member of the NATO alliance in cyber security and in the summer of 2010 signed a Memorandum of Understanding for Cooperation in Cyber Defence with NATO. It participates in various NATO cyber exercises such as Cyber Coalition, Crisis Management Exercise CMX, and others.

3.4. Cyber crisis management

Lithuania does not currently have an overarching crisis management law that clearly recognises a crisis caused by a cyber incident or cyber attack. The crisis management system in Lithuania currently works through the relevant ministries and institutions according to their competencies. The recently passed Law on Cyber security supports the interpretation that in the case of a cyber incident or cyber-attack of national security

[48] Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (Cyber security law of the Republic of Lithuania 11 December 2014 Nr. XII-1428, II-8.2. https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.

[49] Lietuvos kriminalinės policijos biuras.

[50] Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (Cyber security law of the Republic of Lithuania 11 December 2014 Nr. XII-1428, II-12. https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.

[51] ibid. II-12-3.

[52] Lithuanian: Valstybinės duomenų apsaugos inspekcijos. State Data Protection Inspectorate, https://www.ada.lt/go.php/lit/English/3.

[53] Law on the Legal Protection of Personal data, Article 36 p. 1. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=435305&p_query=&p_tr2=2.

[54] Implementation plan for the first approved strategy was approved in 2010 and the IP for updated strategy was approved in 2014.

[55] Gynybos politika (Defence policy) http://www.kam.lt/lt/gynybos_politika_490.html.

[56] Lithuanian: Kibernetinio saugumo ir telekomunikacijų tarnyba prie KAM.

consequence one of the leading ministries would be the Ministry of National Defence. The Government has created a crisis management committee and the crisis management coordination function is performed by the Prime Minister's Council.[57] In 2012 the Government approved the concept for the Law on Crisis Management (at the time of writing this had not been adopted) in order to create a more effective crisis management system fully integrated with NATO and European Union crisis management systems for the monitoring of potential crisis events, preparation of preventative measures, and more effective execution of crisis identification, reaction and recovery measures.[58]

Lithuania, led by the Crisis management division of the Prime Minister's Office, actively participates in NATO-wide crisis management exercises (CMX). Cyber incidents have been tested in scenarios that included critical infrastructure in CMXs in 2012[59] and 2015.[60] It would seem, however, that after the passage of the Cyber Security Law and establishment of the National Cyber Security Centre some post-law clarification in the form of a Government decree or passage of the proposed Law on Crisis Management is needed in order to clarify the roles and responsibilities of the Prime Minister's Office and Cyber Security Centre during a crisis or extreme event caused by a cyber-incident.

3.5. Cyber intelligence

Intelligence and counter intelligence in Lithuania are covered under the Intelligence Law.[61] Under the law intelligence activities are carried out by the State Security Department (accountable to the President and Seimas) and the Second Operative Investigations Department (SOID)[62] under the Ministry of National Defence.[63] In 2015 the State Security Department issued its report on *Threats to National Security* where cyber threats to Lithuania's national security are covered.[64] Information collection about cyber threats is included as part of the National Defence System Cyber Security Strategy Implementation Plan approved by the Minister of National Defence. Information from open sources about cyber incidents and potential cyber threats to critical infrastructure are to be collected and summarised in reports on a regular basis. The institutions at the MoND contributing to this effort are Strategic Communications Department of the Lithuanian Armed Forces, the Joint Defence Staff, SOID and the CTS under the MoND.[65]

3.6. Private sector involvement

Private sector involvement and cooperation with industry, popularly called a 'public-private partnership' (PPP), in the area of cyber security is an on-going process in Lithuania. In the past task forces and work groups representing public and private sector entities have been created to deal with specific questions. For example in order to address concerns over responding to cyber incidents during Lithuania's presidency of the European

[57] Lietuvos Respublikos 2012 m. gegužės 29 d. nutarimas Nr. 633 dėl krizių valdymo įstatymo koncepcijos patvirtinimo IV-5 (Government 29 May 2012 decree Nr. 633 on approval of a Concept for Law on Crisis management) https://www.e-tar.lt/mobile/legalAct.html?documentId=TAR.9871F332B956.

[58] ibid. II-3.

[59] NATO conducts annual crisis management exercise (CMX) and cyber coalition exercise, Press Release (2012) 131 issued on 31 Oct. 2012, http://www.nato.int/cps/en/natolive/news_91115.htm?mode=pressrelease.

[60] NATO conducts Annual Crisis Management Exercise (CMX) http://www.nato.int/cps/en/natohq/news_117862.htm.

[61] Lietuvos Respublikos žvalgybos įstatymas (17 July 2000) Nr. VIII-1861 (Intelligence Law of the Republic of Lithuania) http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=494190.

[62] Lithuanian: Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos.

[63] Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos statuto įstatymas (Law on statute of second operational service department under the MoND) 20 January 2006 d. Nr. X-505, III -8-1. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=270353&p_query=Antrojo%20operatyvini%F8%20tarnyb%F8%20departamento%20prie%20Kra%F0to%20apsaugos%20ministerijos&p_tr2=2.

[64] Grėsmių nacionaliniam saugumui vertinimas (Evaluation of Threats to National Security) http://www.vsd.lt/Files/Documents/635633000992101250.pdf, 7.

[65] Minster of National Defence 19 March 2014 Order Nr. V-220 approving the National Defence System Cyber security Strategy implementation plan for 2014-2015. 5.1.1.

Council in the second half of 2013, the MoI created a temporary Cyber Security Incident Management Group composed of public and private entities tasked with responding to cyber emergencies.[66] The Academy of Science of Lithuania held a conference in November of 2014 on national cyber security which included expert representatives from the public, private, and academic sectors.[67] The Cyber Security Council is potentially a major instrument for further promoting this partnership and cooperation; its first meeting took place on July 21 at the MoND.[68] Time will tell what form and scope of partnership and cooperation will be achieved under this framework.

Closing remarks

Lithuania's cyber security institutions and management of cyber threats have gone through a long evolution, starting from the creation of the first institutions dealing with cyber security to the recent over-arching law on Cyber Security. Lithuania has built up a capable capacity for dealing with its own cyber security concerns. However this is not enough to address all the issues; there is the potential to do more. This capacity should not be limited to dealing with just domestic cyber security questions, but should also be applied to cooperation with Lithuania's neighbours in cyberspace. Among the challenges facing Lithuania are raising awareness about the dynamic threats emanating from cyberspace and insuring the availability of trained cyber security professionals. The newly created cyber security institutions need specialists trained in dealing with today's cyber threats, both in the public and private sectors.

[66] 2013-07-24. Gerinamas kibernetinio saugumo incidentų valdymo koordinavimas (Improving cyber security incident coordinated Response) http://www.ird.lt/blog/2013-07-24-gerinamas-kibernetinio-saugumo-incidentu-valdymo-koordinavimas/.

[67] LMA Technikos mokslų skyrius surengė diskusiją 'Kibernetinis saugumas '(Lithuanian academy of science technology division holds discussion 'Cyber security', 2014. http://www.mokslasirtechnika.lt/mokslo-naujienos/lma-technikos-moksl-skyrius-sureng-diskusija-kibernetinis-saugumas.html.

[68] Cyber Security Council of Lithuania convened for the first time 2015.07.21 http://www.kam.lt/en/news_1098/current_issues/cyber_security_council_of_lithuania_convened_for_the_first_time.html .

References

About CERT-LT, https://www.cert.lt/en/index.html.

Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos statuto įstatymas, 20 January 2006 d. Nr. X-505, III -8-1. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=270353&p_query=Antrojo%20operatyvini%F8%20tarnyb%F8%20departamento%20prie%20Kra%F0to%20apsaugos%20ministerijos&p_tr2=2.

Country (Lithuania) profiles, the relative position against all other European countries. http://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={"indicator-group":"egovernment","ref-area":"LT","time-period":"2014"}.

Cyber Security Council of Lithuania convened for the first time 2015.07.21 http://www.kam.lt/en/news_1098/current_issues/cyber_security_council_of_lithuania_convened_for_the_first_time.html.

Dėl elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudojimo tvarkos aprašo patvirtinimo 2015 m. gegužės 26 d https://www.e-tar.lt/portal/lt/legalAct/f984390005c011e588da8908dfa91cac.

Digital agenda for Europe, Country profiles, the relative position against all other European countries, eCommerce indicators (Lithuania) 2014 http://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={"indicator-group":"ecommerce","ref-area":"LT","time-period":"2014"}.

Elektroninio deklaravimo Sistema, http://deklaravimas.vmi.lt/lt/Pradinis_Prisijungimo_puslapis/Prisijungimasperisorinessistemas.aspx.

Gerinamas kibernetinio saugumo incidentų valdymo koordinavimas 2013-07-24, http://www.ird.lt/blog/2013-07-24-gerinamas-kibernetinio-saugumo-incidentu-valdymo-koordinavimas/.

Government 29 June 2011 Resolution Nr. 796. II-(6.1 – 6.3) Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais program, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=403385.

Grėsmių nacionaliniam saugumui vertinimas, http://www.vsd.lt/Files/Documents/635633000992101250.pdf.

Gynybos politika, http://www.kam.lt/lt/gynybos_politika_490.html.

Hosting Services, http://www.webopedia.com/TERM/H/hosting_services.html.

InComSystems, Plačiajuosčio ryšio infrastruktūros plėtros ir paslaugų naudojimo skatinimo modelio parengimo paslaugų galutinė ataskaita, 2014, http://www.ivpk.lt/uploads/Leidiniai/Galutinė%20ataskaita.pdf.

Istorija IVP, http://www.ivpk.lt/lthm/istorija.

L. Telksnys, A. Žilinskas, ‘Computers in Lithuania’, IEEE Annals of the History of Computing, Vol. 21, No. 3, 1999 http://www.mii.lt/files/telk_zil_annals.pdf.

Law on the Legal Protection of Personal data, Article 36 http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=435305&p_query=&p_tr2=2.

Lietuvos e sveikatos sistema pradeda veikti, http://www.15min.lt/naujiena/aktualu/sveikata/lietuvos-e-sveikatos-sistema-pradeda-veikti-541-507348.

Lietuvos gyventojų mokėjimo įpročių apklausos apžvalga 2014, Bank of Lithuania ISSN-2335-81302 (online) 2015-08-27, http://www.lb.lt/lietuvos_gyventoju_mokejimo_iprociu_apklausos_apzvalga_1.

Lietuvos Respublikos 2012 m. gegužės 29 d. nutarimas Nr. 633 dėl krizių valdymo įstatymo koncepcijos patvirtinimo IV-5 https://www.e-tar.lt/mobile/legalAct.html?documentId=TAR.9871F332B956.

Lietuvos Respublikos elektroninio parašo įstatymas, https://www.e-tar.lt/portal/lt/legalAct/TAR.382345294FBF/TAIS_463802.

Lietuvos Respublikos elektroninių ryšių įstatymas, 2004 april 15 Nr. IX-2135 (II-(6-9)) http://www3.lrs.lt/pls/inter3/oldsearch.preps2?Condition1=232036&Condition2=.

Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428, 11 December 2014 Nr. XII-1428, II-10.11-4. https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.

Lietuvos Respublikos Ministro Pirmininko 2008-06-17 potvarkiu Nr. 225 sudarytos darbo grupės pasiūlymams dėl Lietuvos kibernetinio saugumo stiprinimo krypčių ir priemonių rengti veiklos ataskaita (Prime Minister‘s 2008-06-17 tasking Nr. 225 Workgroup report on recommmended course and measures for strengthening cyber security in Lithuania).

Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas 1996 m. gruodžio 19 d. Nr. VIII-49, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=442449.

Lietuvos Respublikos Seimas nutarimas dėl nacionalinio saugumo strategijos patvirtinimo 2002 m. gegužės 28 d. Nr. IX-907, III. 8.8, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=429234.

Lietuvos Respublikos žvalgybos įstatymas (17 July 2000) Nr. VIII-1861, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=494190.

Lithunian National Communications Regulatory Authority Report on the electronic communications sector Quarter IV, 2014, 30. http://www.rrt.lt/en/reviews-and-reports/reports-on-the-urpp/2014_1098.html Updated on 2015-04-24.

LMA Technikos mokslų skyrius surengė diskusiją „Kibernetinis saugumas ', 2014. http://www.mokslasirtechnika.lt/mokslo-naujienos/lma-technikos-moksl-skyrius-sureng-diskusija-kibernetinis-saugumas.html 2015-08-27.

LR Vyriausybes pasitarimo protokolas 2009 m. balandžio 15 d. Nr. 29 18. Dėl LR Ministro Pirmininko 2008 m. birželio 17 d. potvarkio Nr. 225 sudarytos darbo grupės Lietuvos kibernetinio saugumo klausimams išnagrinėti ir pasiūlymams dėl jo stiprinimo parengti pasiūlymo įgyvendinimo.

LRV 2015 m. balandžio 23 d. Nutarimas Nr. 422 Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo, https://www.e-tar.lt/portal/lt/legalAct/4e3539f0ee4611e4927fda1d051299fb.

Minster of National Defence 19 March 2014 Order Nr. V-220 approving the National Defence System Cyber security Strategy implementation plan for 2014-2015. 5.1.1.

Nacionalinis kibernetinio saugumo centras, http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/rysiu_ir_informaciniu_sistemu_tarnyba_prie_kam_2482/nacionalinis_kibernetinio_saugumo_centras.html.

NATO, NATO conducts annual crisis management exercise (CMX) and cyber coalition exercise, Press Release (2012) 131, issued on 31 Oct. 2012, http://www.nato.int/cps/en/natolive/news_91115.htm?mode=pressrelease.

NATO, NATO conducts Annual Crisis Management Exercise (CMX) http://www.nato.int/cps/en/natohq/news_117862.htm.

Populiariausios paslaugos, https://www.epaslaugos.lt/portal/.

Projekto prielaidos, http://placiajuostis.lt/lt/projekto-prielaidos2.

RAIN broadband internet project website, http://placiajuostis.lt 2015-08-27.

Ryšių reguliavimo tarnybos 2015-03-31 LR Electroninio parašo įstatymo įgyvendinimo 2014 metų ataskaita, http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroninio-paraso-istatymo-1b73.html.

State Data Protection Inspectorate. https://www.ada.lt/go.php/lit/English/3.

Strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas, 20 October 2002 Nr. IX-1132.

Šviesolaidinė infrastruktūra http://placiajuostis.lt/lt/sviesolaidine-infrastruktura2.