CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cyber Security Organisation: CZECHIA

Tomáš Minárik
Revised and updated by Taťána Jančárková

National Cyber Security Governance Series

Tallinn 2019

About this study

This publication is part of a series of country reports offering a comprehensive overview of national cyber security governance by nation. The aim is to improve awareness of cyber security management in the varied national settings, support nations enhancing their own cyber security governance, encourage the spread of best practices, and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO Nations that are Sponsoring Nations to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), each country report outlines the division of cyber security roles and responsibilities between agencies, describes their mandate, tasks, and competences as well as coordination between them. In particular, it covers 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 management. It offers an introduction to the broader digital ecosystem of the country and outlines national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 25 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts in Tallinn the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. As of January 2018, CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations, currently Austria, Belgium, Bulgaria, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. The NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence. It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

Reports in this series

National Cyber Security Organisation in Czechia

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in Turkey

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation in Israel

Series editor: Kadri Kaska (NATO CCDCOE)

Information in this document has been checked for accuracy as of October 2019.

Table of Contents

Country indicators

10.6 million	Population
9.3 million (88.4%)	Internet users (% of population)
78.9 thousand	Area (km²)
39.7 thousand	GDP per capita (USD)

International rankings*

43th	ICT Development Index (ITU 2017)
54th	E-Government Development Index (UN 2018)
18th	Digital Economy and Society Index (EU 2019)
71th	Global Cybersecurity Index (ITU 2018)
1st	National Cyber Security Index (eGA 2019)

1. Digital society

1.1 Infrastructure availability and take-up

Basic fixed broadband is available to nearly every Czech household, with the coverage remaining constant at around 98% since 2014.[1] In 2018, 86% of households had internet access at home and 84% of the population were regular internet users (cf. 79% and 77%, respectively, in 2015). The fixed broadband take-up was 74% of households[2] or 30.4 subscriptions per 100 people.[3] Of the broadband subscriptions in 2018, 18% enabled download speed of 100 Mbps (ultrafast broadband) and 37% enabled at least 30 Mbps (fast broadband), which represented an increase by 13 and 11 percentage points, respectively, from 2014.

Mobile 4G broadband coverage has increased from 92% of the population in 2014 to 99% in 2018, while mobile broadband take-up has advanced from 62.3 subscriptions per 100 people in 2014 to 82.4% in 2018.[4]

* International rankings rely on varied methodology and sources for their scores.

[1] Unless explicitly stated otherwise, the statistics in this section are taken from the EU Digital Agenda Scoreboard, 'Digital Economy and Society Index, Country Profile: Czech Republic', https://ec.europa.eu/digital-agenda/en/scoreboard/czech-republic.

[2] 'Countries' performance in digitisation', European Commission, http://ec.europa.eu/digital-single-market/en/progress-country.

[3] https://digital-agenda-data.eu/charts/see-the-evolution-of-an-indicator-and-compare-countries#chart={%22indicator-group%22:%22any%22,%22indicator%22:%22bb_penet%22,%22breakdown%22:%22total_fbb%22,%22unit-measure%22:%22subs_per_100_pop%22,%22ref-area%22:[%22CZ%22,%22EU28%22,%22EU27%22]}.

[4] https://digital-agenda-data.eu/charts/see-the-evolution-of-an-indicator-and-compare-countries#chart={%22indicator-

The first 5G spectrum auction has been announced to take place in the second half of 2019, final conditions, however, are yet to be confirmed.

The data shows that internet penetration has been steadily growing, although at a relatively slow pace. All of these figures are close to the EU averages, nonetheless. It is worth noting, however, the comparatively low mobile internet take-up, perhaps due to mobile data prices which are among the highest in Europe.[5]

1.2 Digital public services

Despite a legislative framework in place since 2009,[6] Czechia has had mixed success in implementing a comprehensive e-governance agenda. In particular, major discrepancies have been continuously observed between the use of digital public services by private individuals as compared to businesses. This is probably due to the fact that all legal persons were provided with a free but obligatory 'data mailbox'[7] from 1 July 2009 onwards. The data mailbox works as a normal email account, but it provides for the authenticity and non-deniability of data stored (using the SHA-2 hash function algorithm), thereby eliminating the need for a separate certificate for electronic signatures. Any official correspondence between legal persons and authorities is restricted to the data mailbox. As any unread messages delivered to the data mailbox are considered to have been read by the addressee 10 days after delivery, enterprises have little choice but to comply with e-governance procedures surrounding the use of the data mailbox. Conversely, natural persons are under no obligation to use the data mailbox and the offer of e-government services remains limited; consequently only few have it (according to media accounts, around 2% in 2018 and less than 1% in 2014).[8]

Certificates for electronic signatures are not provided by public authorities and must be purchased from commercial entities, which has become another obstacle to the more widespread use of e-government by natural persons. Nevertheless, after a stagnation in 2017, the share of e-government users grew by 19 percentage points to 52% by 2019. Correspondingly, Czechia's ranking in the digital public services category grew from 25th place among EU member states in 2015 to 20th place in 2019.[9]

The new e-government strategy (*Digitální Česko: Informační koncepce České republiky*) was adopted in 2018.[10] It lists five objectives: 1) more effective and user friendly online services for citizens and businesses; 2) digital friendly legislation; 3) favourable conditions for the use of digital technologies in public services; 4) digital skills for public officials; and 5) central coordination of public services' ICT development. As of July 2018, Czechs can use new e-ID cards with chips and receive certain public services over the internet. 570,000 people had the new e-ID card at the end of 2018. As of January 2018, mandatory electronic prescriptions were introduced in the healthcare sector.

group%22:%22any%22,%22indicator%22:%22mbb_penet%22,%22breakdown%22:%22total_mbb%22,%22unit-measure%22:%22subs_per_100_pop%22,%22ref-area%22:[%22CZ%22,%22EU28%22,%22EU27%22]}.

[5] DESI Report 2019 – Connectivity, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60010, European Commission, Mobile Broadband Prices in Europe 2018 report, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57336.

[6] Act No. 300/2008 Coll., on electronic acts and conversion of authorised documents, in effect since 1 July 2009.

[7] Datoveschranky.info, 'Datové Schránky', 2014, https://www.datoveschranky.info/.

[8] Správa základních registrů, 'Roční výpisy o využívání údajů v registru obyvatel a registru osob, Správa základních registrů', 2014, http://www.szrcr.cz/zakladni-registry-dale-zvysuji-transparentnost-verejne.

[9] DESI Country Profile, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59889.

[10] Rada vlády pro informační společnost, https://www.mvcr.cz/clanek/rada-vlady-pro-informacni-spolecnost.aspx

In 2018, the Czech government also appointed a Chief Digital Officer for IT and Digitisation charged with coordinating the implementation of strategy.

In 2019, the government adopted the National Artificial Intelligence Strategy.[11] Its main objective is to support the concentration of research and development (R&D) in artificial intelligence (AI), in particular by supporting the creation of the European Centre of Excellence, Test Centre and Digital Innovation Hubs. The strategy further aims at a deeper cooperation with global AI centres, maintaining intellectual potential at home and simplifying conditions for attracting top foreign talent through research funding, development of start-ups, availability of resources for innovation of SMEs and economy development. The state should primarily contribute by making available data, completing digital infrastructure, supporting the transformation of enterprises and introducing modern public administration services, introducing clear legislation, investor security and international cooperation along with adequate education and training, both technical and non-technical.

1.3 Digitisation in business

Czechia had a relatively high proportion of turnover from e-commerce at 30% in 2015, which almost doubled the EU average and placed the country in 2nd place among EU member states. The share of the internet-based economy was estimated at 4.13% of GDP in 2015, with that of the ICT sector as a whole being 3.85% of GDP.[12]

Some 67% of all individuals ordered goods or services online in 2018 (compared to 45% in 2015), which generally coincides with the EU average (14th place). Czech small and medium enterprises (SMEs) ranked among the top 5 in selling online (23% in 2018), selling online cross-border (12% in 2017) and the share of e-commerce on SME total turnover (18% in 2018). The e-commerce sector appears to develop mainly at the national level; while figures for internet purchases are at the EU average or even slightly above, the online cross-border purchases by individuals remain at less than half of the EU average.[13]

Overall, Czechia is well digitised and consequently dependent on the use of ICT. Its commercial sector is doing particularly well with respect to the internet economy, and further growth is expected. However, more effort could be put into translating Czechia's enthusiasm for e-commerce into a higher uptake of e-government services by citizens.

[11] National Artificial Intelligence Strategy of the Czech Republic, https://www.mpo.cz/assets/en/guidepost/for-the-media/press-releases/2019/5/NAIS_eng_web.pdf.

[12] 'Studie SPIR - Česká internetová ekonomika', 2013, 2016 http://www.studiespir.cz (Czech Internet Economy Study 2013, 2016, in Czech)

[13] European Commission, Digital Scoreboard Visualisations, https://digital-agenda-data.eu/charts/see-the-evolution-of-an-indicator-and-compare-countries#chart={%22indicator-group%22:%22any%22,%22indicator%22:%22i_bfeu%22,%22breakdown%22:%22ind_total%22,%22unit-measure%22:%22pc_ind%22,%22ref-area%22:[%22CZ%22,%22EU28%22,%22EU27%22]}.

2. National cybersecurity strategy and legal framework

2.1 National strategy

Czechia's current *National Cyber Security Strategy* (NCSS)[14] and the associated *Action Plan* (AP)[15] were drafted by the Czech National Security Authority (NSA, *Národní bezpečnostní úřad*)[16] and adopted by the Government in 2015.[17] Both cover the years 2015 to 2020. The previous NCSS and AP covered the years 2012 to 2015.[18] Preparatory process for a new national strategy began in April 2019 under the auspices of the new NSA-derived national authority, the National Cyber and Information Security Agency (NCISA, *Národní úřad pro kybernetickou a informační bezpečnost*),[19] and the draft strategy should be ready for intragovernmental review by the end of the year. The draft action plan shall follow suit.

Cyber security strategy objectives

Building on the achievements of the 2012-2015 NCSS, the main objectives of which were to create a legislative framework of cyber security and to establish the National Cyber Security Centre (NCSC, *Národní centrum kybernetické bezpečnosti*) and Governmental CERT (see details in Section 3.2.), the current NCSS pursues enhanced models of cyber security development. This translates into a set of visions, principles, challenges and main goals identified as a reflection of Czechia's aspiration to 'play a leading role in the cyber security field within its region and in Europe' and, amongst others, the focus on 'securing industrial control systems included in the [critical information infrastructure] and within a few years [becoming] one of the leading nations in this area by virtue of the expertise and knowledge acquired'.[20] Another fairly progressive objective is the protection of the right of the individual to informational self-determination, which underlies the thinking behind the cyber security regulatory framework.[21]

[14] 'Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020', 2015 http://www.govcert.cz/download/nodeid-1004/ (the original Czech version); 'National Cyber Security Strategy of Czechia for the Period from 2015 to 2020', 2015 http://www.govcert.cz/download/nodeid-1075/ (in English).

[15] 'Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020', 2015, http://www.govcert.cz/download/nodeid-973/ (the original Czech version); 'Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020', 2015 http://www.govcert.cz/download/nodeid-590/ (in English).

[16] National Security Authority, http://www.nbu.cz/en/.

[17] National Cyber Security Centre, http://www.govcert.cz/en/info/events/the-government-of-the-czech-republic-adopted-the-national-cyber-security-strategy-for-the-upcoming-five-years/, http://www.govcert.cz/en/info/events/the-government-adopted-the-action-plan-to-the-national-cyber-security-strategy-for-subsequent-5-years-and-the-2014-status-report-on-the-cyber-security-in-the-czech-republic/.

[18] 'Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015', 2012 http://www.govcert.cz/download/nodeid-727/ (the original Czech version); 'Strategy of the Czech Republic in the field of Cybernetic Security for 2012 - 2015', 2012 http://www.govcert.cz/download/nodeid-1190/ (in English). 'Akční plán ke strategii pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015', 2012, http://www.govcert.cz/download/nodeid-896/ (the original Czech version; no translation is available).

[19] www.nukib.cz.

[20] NCSS, p. 7.

[21] NCSS, p. 9.

Strategic goals and tasks

The NCSS sets out eight strategic goals. Specified tasks for the furtherance of these goals are defined by the Action Plan. The following is a representative but non-exhaustive summary of the goals and tasks. The current status of their implementation is outlined in the subsequent section.

A. Efficiency and enhancement of all relevant structures, processes, and of cooperation in ensuring cyber security

This goal comprises the improvement of communication and cooperation among the relevant cyber security actors (CERT and CSIRT teams, central authorities), both domestic and international. Czechia plans to '[d]evelop a national coordinated incident handling procedure that will set a cooperation format, contain a communication matrix, a procedure protocol and define each actor's role', and a national risk assessment methodology in accordance with the requirements introduced by the Act on Cyber Security and its implementing regulations. The task of carrying out national cyber security exercises is also included under this goal.

B. Active international cooperation

This explicitly covers the EU (including ENISA), NATO (including NATO CCDCOE), OSCE, UN (including ITU), the Visegrad Four countries and the Central European Cyber Security Platform, and bilateral cooperation, including the CERT/CSIRT teams, international organisations and academic centres. Czechia will also participate in international discussions on internet governance and on international legal norms in cyberspace. The task of participating in and organising international exercises is included under this goal.

C. Protection of national critical information infrastructure (CII) and important information systems (IIS)

Czechia will continue identifying and supporting the entities operating critical information infrastructure and important information systems, in accordance with the Act on Cyber Security. It will support the creation of new CERT/CSIRT teams in Czechia. It plans to develop its own capacities and capabilities for cyber security testing, forensic analysis, malware detection and testing, and to implement a honeypot system for cyber threat detection.

The country intends to draft a National Cloud Computing Strategy and create a secure state cloud, including data storage.

The number of personnel of specialised intelligence services units and of the Government CERT should increase in order to improve their threat detection and analysis capabilities, and solutions for improved and automated information sharing between the state and CII and IIS entities should be implemented.

This heading of the NCSS also describes the establishing of National Cyber Forces Centre (*Národní centrum kybernetických operací*)[22] within Military Intelligence to be able to perform a wide range of operations in cyberspace and other activities necessary for ensuring the state's cyber defence, including in support of international military operations by EU or NATO, or to defend Czechia in a hybrid conflict. Notably, Czechia will '[t]rain experts specialised in questions of active counter-measures in cyber security and cyber defence and in offensive approach to cyber security in general'.

Finally, a procedure will be developed for the transition from the state of cyber emergency, as defined by the Act on Cyber Security, to the general crisis states defined in Constitutional Act No. 110/1998 Coll., on the Security of Czechia.

[22] See Chapter 3.3 on NCOC below.

D. Cooperation with private sector

This topic comprises the coordination of IPv6 transition, supporting the spreading of DNSSEC, educating the public about cyber security, and creating an information-sharing platform for the NCSC and the CII and IIS entities.

E. Research and development / Consumer trust

By Q3 2018, the NCSC will prepare the national cyber security research and development concept, in cooperation with other agencies and stakeholders. It will also continuously plan, initiate, and cooperate on the implementation of the research projects, helping to involve Czech academia and the private sector in international research programmes.

F. Education, awareness raising and information society development

This topic comprises awareness raising both among students and the public at large. By the beginning of 2017, primary and secondary school curricula should be modernised with respect to cyber security, methodical materials provided, and teachers trained. Also, new university study programmes on cyber security should be created and the existing ones promoted. Public administration personnel should also be trained in cyber security.

G. Support to the Czech Police capabilities for cybercrime investigation and prosecution

By 2018, the cybercrime departments of the Czech Police should be reinforced, both at the central and regional levels, and the technological equipment of specialised police departments should be modernised. Direct links should be established at the working level with the intelligence services, NCSC, and both Government CERT and National CERT. Police experts should receive professional training in cyber security.

H. Cyber security legislation (development of legislative framework). Participation in creation and implementation of European and international regulations

Czechia should actively participate in the drafting and implementation of relevant EU and international law. Cyber security legislation (both laws and regulations) should be kept up to date. In particular, cybercrime investigation and prosecution should be made more effective by updating the relevant laws. Cyber security training should be provided to judges and prosecutors so that they can better handle cybercrime cases.

Interim review of the strategy implementation

The NCSS implementation is subject to regular review; every six months the interdepartmental working group (see below) evaluates the level of achievement of individual tasks and can adjust the action plan accordingly. A report on NCSS implementation is appended to the annual Report on Cyber Security prepared by NCISA. Although unclassified, the implementation report is not released to the public.

Overall, the implementation of the national strategy can be deemed satisfactory. In some areas, the results have exceeded expectations, in others, delays have been noted, as is the case, for instance, with the national cyber security research and development concept. Due to be complete in 2018, preparatory works were still going on in July 2019. Nevertheless, thanks to an increase in dedicated human resources, it was expected that all research and development related targets would be met by the end of the strategy implementation. A dedicated department has been created within NCISA, integrating competencies for research and development as well as education related tasks such as the national education concept, e-learning module for public administration and the previously introduced pilot courses at secondary and higher education establishments.

In 2016, a *Strategic Framework for the National Cloud Computing* (*Strategický rámec Národního cloud computingu – eGovernment cloud ČR*)[23] was adopted and a Working Party on eGovernment Cloud was convened to analyse the capacities and prepare implementation of the eGovernment Cloud due to begin in 2019 and a feasibility study for the eGovernment Portal.[24]

Similarly, institutional cooperation in fighting cybercrime gained momentum in early 2019 when a memorandum was signed by the Police of Czechia, the Prosecutor General's Office and NCISA to set out rules for cooperation, to identify respective competencies, and to ensure information sharing and collaboration on training and exercices.

Cyber security exercises have over the past few years become one of the cornerstones of Czechia's cyber security organisation structure and an important export commodity. By 2019, Czech teams comprising government, industry and academia members have successfully participated in major international cyber security and crisis management exercises including Locked Shields,[25] Cyber Coalition, CMX and Cyber Europe. NCISA has been also able to repeatedly deliver customised exercises to international audiences as varied as the US Congress, countries of the African Union and national authorities in the Western Balkans.

Czechia has also been active in other areas of international cooperation. On 12 October 2015, Czechia, represented by the NSA, became the first NATO member state to sign a 'second generation' Memorandum of Understanding on cyber defence cooperation with NATO's Cyber Defence Management Board.[26] It actively participated in multilateral negotiations on an EU cyber security regulatory framework, election security, implementation of confidence-building measures for cyberspace and various capacity-building platforms.

In respect of cooperation with the private sector, NCISA and Microsoft signed a new security program in 2018, focusing primarily on information sharing and exchange. A Memorandum of Understanding also exists with Cisco and was signed in 2016 (see section 3.5).

2.2 Legal framework

The cornerstone of Czechia's cyber security legislative framework, the Act on Cyber Security and Change of Related Acts (Act no. 181/2014 Coll.), came into force on 1 January 2015[27] and is complemented by a set of implemented regulations that took effect on the same date.[28] It defines several

[23] https://www.databaze-strategie.cz/cz/mv/strategie/strategicky-ramec-narodniho-cloud-computingu-egovernment-cloud-cr (in Czech).

[24] https://www.isss.cz/archiv/2019/download/prezentace/mvcr_tuma.pdf (in Czech)

[25] The Czech team became the overall winner in 2017 and finished in the top 3 in 2018 and 2019.

[26] NATO, 'NATO and Czechia bolster cyber defence cooperation', http://www.nato.int/cps/en/natohq/news_123857.htm.

[27] 'Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)', https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/ (in Czech); https://www.govcert.cz/en/legislation/legislation/ (in English).

[28] These are:

- Government Regulation No. 315/2014 Coll. Amending Government Regulation No. 432/2010 Coll. on the Criteria for the Determination of the Elements of the Critical Infrastructure;
- Regulation No. 316/2014 Coll. on Cyber Security; replaced by regulation No. 82/2018 Coll. on Cyber Security
- Regulation No. 317/2014 Coll. on Important Information Systems and Their Determining Criteria
- Regulation No. 437/2017 Coll. on Criteria for the Determination of Operators of Essential Services

See n. 27 above for links.

categories of regulated entities and defines their legal obligations and the competencies of the NCISA as the national authority.

Those categories generally are, in descending order reflecting the extent of imposed legal obligations:

(i) operators of systems of critical information infrastructure;

(ii) operators of essential services;

(iii) operators of important information systems;

(iv) digital service providers;

(v) providers of electronic communication services or operators of electronic communication networks; and

(vi) operators of important networks as defined by law.

The act originally built on the legislation pertaining to protection of critical infrastructure and crisis management,[29] thus inscribing critical information infrastructure protection into a larger framework of critical infrastructure protection and by inference imposing obligations also under crisis management regulations. Following the adoption of the EU Directive on Security of Network and Information systems (the NIS directive) in 2016, a new category of obliged entities has been added (operators of essential services) which only bore cyber security related obligations. The two subsequent categories, covering certain types of information systems and networks in public administration sector and select information society services, carry a substantially lighter burden, with security measures largely dependent on their own risks assessment. The remaining categories are principally regulated by electronic communications law and carry only marginal obligations pursuant to the Cyber Security Act.

Generally speaking, obligations and security measures under Cyber Security Act relate to risk management, security of assets, supply chain security, public procurement or incident management. Select obligations and security measures are further outlined in Chapter 3 below.

3. National cybersecurity governance

3.1 Policy coordination and setting strategic priorities

Government Resolution no. 781 of 19 October 2011 entrusted the NSA with coordination responsibility for cyber security in Czechia. The same Resolution established the National Cyber Security Centre (NCSC, *Národní centrum kybernetické bezpečnosti*), which was subordinated to the Czech NSA and tasked with: operation of the Government CERT; cooperation with CSIRTs, both national and international; preparation of security standards for various categories of entities in Czechia; support to education and the raising of cyber security awareness; and support to cyber security research and development.

Following a 2017 administrative overhaul, overall responsibility for national cyber security has gone to a dedicated agency. The **National Cyber and Information Security Agency** (NCISA, *Národní úřad pro kybernetickou a informační bezpečnost*)[30] that, by virtue of Government Resolution no. 1178 of 19 December 2016 and the subsequently amended Act on Cyber Security derived from the NSA, became

[29] Act no. 240/2000 Coll., on crisis management, and Government Regulation no. 432/2010 Coll., on Criteria for the Determination of the Elements of the Critical Infrastructure.

the coordinating authority for cyber security as of 1 August 2017. NCISA comprises the NCSC and select elements of the NSA that dealt with security of classified information systems.

The new agency has seen the staff numbers rise to almost 200 by early 2019 which is in line with the Government Resolution no. 1049 of 28 November 2016 envisaging a gradual budget growth and increase in personnel as well as building new agency premises.

Government Resolution no. 781 of 19 October 2011 also established the **Cyber Security Council** (CSC, *Rada pro kybernetickou bezpečnost*),[31] which is the official forum for interagency coordination.[32] The CSC includes representatives from the Czech NCISA, the Ministry of Interior, the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Finance, the Ministry of Industry and Trade, the Ministry of Transport, the Police, the Office for Foreign Relations and Information (the external civilian intelligence service), the Security Information Service (the internal civilian intelligence service), Military Intelligence, the Office for Personal Data Protection, and the Czech Telecommunications Office. According to need, the CSC may invite representatives of entities operating critical infrastructure or external experts to participate in its meetings.

Two interdepartmental working groups on the coordination of cyber security were established within the CSC in November 2015. The first deals with national cyber security issues, including regular evaluation of fulfilment of the Action Plan. The second covers international issues.

The CSC was complemented by the **Committee on Cyber Security** (*Výbor pro kybernetickou bezpečnost*) in 2017[33] as one of the regular working bodies within the State Security Council. The cyber security portfolio thus acquired permanent standing within the highest advisory body of the Government.

3.2 Cyber incident management and coordination

Several CERT/CSIRT teams operate in Czechia, both in the public and private spheres.[34] The Cyber Security Act provides for and defines competencies of two of such teams. At the government level there exists the **Government CERT** (GovCERT.CZ)[35] based in Brno, which reached full operational capability at the same time as the NCSC in January 2016. Its main task is to collect reports of cyber incidents from specified entities, analyse them, and provide help. The Cyber Security Act introduced an obligation to report cyber incidents for entities operating critical information infrastructure (CII), important information systems (i.e. other vital systems of public authorities), and internet exchange points enabling direct connection to CII or to a network abroad (i.e. important networks as defined by the Act). Following the transposition of the NIS Directive in 2017, a new category of operators of essential services, whose

[31] https://www.govcert.cz/en/csc/cyber-security-council/.

[32] The Statute of the Cyber Security Council is in the Annex to the Government Resolution no. 781 of 19 October 2011, http://kormoran.odok.cz/usneseni/usneseni_webtest.nsf/0/87725D06F85FE727C1257956002CC333/$FILE/781%20p%C5%99%C3%ADloha%20w111019a.0781.pdf (only available in Czech).

[33] ‘Výbor pro kybernetickou bezpečnost’ in Czech. The Statute and the Rules of Procedure of the Committee are in the Annex to the State Security Council Resolution no. 18 of 3 May 2017, https://www.vlada.cz/cz/ppov/brs/pracovni-vybory/kyberneticka_bezpecnost/vybor-pro-kybernetickou-bezpecnost-159932/ (only available in Czech)

[34] As of July 2019, there were 44 CERT/CSIRT teams listed, accredited or certified by Trusted Introducer, 3 of those being also members of FIRST. Info available at https://www.trusted-introducer.org/directory/teams.html#url=c%3DCZ%26q%3D and https://www.first.org/members/map#country%3ACZ.

[35] 'Govcert.CZ / Národní centrum kybernetické bezpečnosti ČR', http://www.govcert.cz/en/govcertcz/.

legal obligations under the Cyber Security Act largely mirror those of CII operators, was added to the list of entities.

The above liable entities have a duty to implement preventive security measures ranging from physical security to cryptography, and to report cyber incidents to the Government CERT. In simple terms, the latter's constituency is public sector and critical information and essential services elements of the country's infrastructure (both public and private). Other ISPs continue to report cyber incidents to the national CERT (currently **CSIRT.CZ**),[36] which generally speaking services the remainder of the private sector, including digital service providers pursuant to the NIS directive. National CERT also fulfils specified, mainly reporting and support roles in respect of the Government CERT (see also section 3.5).

According to the Cyber Security Act, the Czech NCISA may order the listed entities to take further protective measures. The NCISA can also declare a state of cyber emergency, in which case it might extend these protective measures to private sector ISPs and other operators of electronic communications networks. It has the authority to carry out security audits and impose fines against the listed entities.

Preventive security measures based on the ISO/IEC 27000-series standards that include comprehensive management, organisational, procedural and system security elements, together with obligations to apply different levels of security measures pertaining to specific categories of entities are defined in the implementing regulations that complement Cyber Security Act. The implementing regulations also specify the procedures for the reporting of cyber incidents, both to GovCERT.CZ and to CSIRT.CZ. A report is to follow a predefined form and can be submitted via an e-form on the respective website, via e-mail, data mailbox,[37] specified interface, or on paper.

3.3 Crisis prevention and crisis management

Information infrastructure as critical infrastructure

Key information infrastructure forms part of the critical infrastructure system regulated both by the Cyber Security Act and Act no. 240/2000 Coll., on Crisis Management. The list of critical infrastructure, as defined by Czech law and reflecting the requirements of the EU Council Directive 2008/114/EC, includes communications and information systems in critical sectors such as energy, water management, food and agriculture, health services, transport, communications and information systems, financial and currency markets, emergency services, and public administration.

Under the Cyber Security Act, CII is defined as 'critical infrastructure falling under the CIS sectoral criterion [pursuant to the Crisis Management Act]'.[38] Entities operating CII have certain duties under the Cyber Security Act (see Part 3.2). The responsibilities for CII security, including the resilience procedures, are described by the Cyber Security Act and by its implementing regulations.

Following the adoption of the NIS Directive, two new categories of entities have been added to the purview of the Cyber Security Act. Operators of essential services (OES) are responsible for services dependent on information and communication systems that are critical for the maintenance of societal or economic activities. Providers of digital services, on the other hand, offer specific information society services. The former are subject to obligations equal to those operating critical information infrastructure under the Cyber Security Act, while the latter have more leeway when it comes to their information security, yet have to fulfil certain criteria.

[36] 'CSIRT', http://www.csirt.cz/.

[37] See part 1.2.1. for the description of data mailbox.

[38] § 2 sub (b) of the Cyber Security Act. Zákon o kybernetické bezpečnosti (n **Error! Bookmark not defined.**).

Information systems which are neither CII nor operated by OES but are nevertheless vital for public administration are termed ‘important information systems’ (IIS) by the Act. IIS operators are subject to only about 60% of the obligations imposed by the Act on Cyber Security on CII operators. There were 109 elements of information infrastructure classified as CII, and 171 as IIS as of July 2019. In addition, 27 entities have been identified as OES. The list of particular entities is not public.

Unlike other EU member states, Czechia has opted for an active CII and OES identification approach, assigning the CII and/or OES status upon administrative decision issued in respect of individual entities following an individual assessment of criteria fulfilment made by NCISA in administrative proceedings in cooperation with the entities concerned. Such process is more time and resources consuming than self-identification, yet believed to be more thorough and accurate.

Crisis management

The Cyber Security Act introduced the concept of a limited state of emergency known as a ‘state of cyber emergency’.[39] A state of cyber emergency can be declared when the national interest is endangered on a large scale by a threat to information security or to the security of electronic communications services. It is declared by the Director of the NCISA for a maximum of 7 days, but can be prolonged repeatedly for up to 30 days on each extension.

The Director of the Czech NCISA informs the Government regularly about the measures being taken during a state of cyber emergency. The Director can order those ISPs or entities operating a CII, IIS or a network enabling a direct connection to CII or to a network abroad or OES to introduce specific cyber security measures. The state of cyber emergency can be cancelled by the Director of the NCISA once the threat has passed. If a threat cannot be managed under the framework of the state of cyber emergency, the Government may declare a general state of emergency.

Crisis management procedures are regularly tested at national cyber security exercises developed by NCISA under the label Cyber Czech. The exercises offer both technical and strategic scenarios and are thematically oriented with a different industry sector involved every year.

Internal procedure has been developed by NCISA to manage declaration and implementation of the state of cyber emergency. No such occasion has yet arisen by the time of writing of this report.

3.4 Military cyber defence

The recent years have seen greater attention being paid to cyber defence, including active measures. Along with cyber security, cyber defence is reflected on in the *Security Strategy of the Czech Republic* (2015), the *Long Term Perspective for Defence 2030* (2015), the *Concept of the Build-up of the Armed Forces of the Czech Republic 2025* (2015), *Defence Strategy of the Czech Republic* (2012), and in the White Paper on Defence (2011).

A new Cyber Defence Strategy for 2018-2022 was adopted in 2018.[40] According to the document, Czechia approaches cyber defence as an autonomous and specific discipline within a larger concept of cyber security. It has also joined the ranks of states which have in principle publicly subscribed to the development of offensive cyber capabilities. Cyber defence competencies are distributed between the two entities.

[39] § 21 of the Cyber Security Act. Zákon o kybernetické bezpečnosti (n **Error! Bookmark not defined.**).

[40] http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-kyberneticke-obrany.pdf (in Czech only)

Military cyber defence is the task of the **Communications and Information Systems Agency** (CISA, *AKIS – Agentura komunikačních a informačních systémů*)[41] which is a part of the Support Division which is in turn subordinated to the General Staff of the Armed Forces of the Czech Republic. CISA is responsible for the build-up and development of the Signal Corps of the Armed Forces and the development and operation of CIS within the Armed Forces.

CISA implements national CIS policies within the Armed Forces and the Ministry of Defence (MOD), coordinating the interconnection of these departments' CIS to other governmental CIS and to NATO CIS. A framework memorandum has been concluded between the MOD and Czech NSA as the civilian national cybersecurity authority which includes cybersecurity and other topics of mutual interest.

The CISA directs and provides for operational planning with regard to CIS including deployable CIS assets, and is responsible for static CIS on national territory, including operational measures and requirements during mobilisation. It is also tasked with provisioning CIS support to organic command and control systems, including the headquarters of the Armed Forces, task forces, EU Battle Groups, the Allied Rapid Reaction Corps, the Integrated Rescue System, crisis management and NATO HQs. CISA also gives technical and logistics support to a Deployable Communication Module as the Czech component of NATO's 3rd Signals Battalion, is responsible for CIS training and procurement within the Armed Forces and MOD, and operates a non-public telecommunications network for the Armed Forces and MOD.

The MOD has a Computer Incident Response Capability (CIRC) operated by CISA, which is responsible for cyber defence across the Armed Forces and MOD. The task of the CIRC is the 'proactive identification of security threats and incidents, their analysis and subsequent reporting of the events and solutions to relevant partners'.[42] The CIRC can prepare remedial countermeasures, tools and procedures, and contribute to the awareness of users and managers of CIS, thereby increasing the resilience of CIS and helping to protect data. CIRC also participates in both national and international cyber defence exercises, cooperates with NCIRC and participates in the Malware Information Sharing Platform.[43]

In 2018, the General Staff decided to develop, from 2019, a new **Cyber and Information Operations Command** (*Velitelství kybernetických sil*) that would incorporate the existing CIRC capabilities and further expand the army's capabilities with regard to protection of military operations and mission assurance.[44]

As regards active cyber defence, it is mentioned abundantly in the NCSS and AP,[45] and the **National Cyber Operations Centre** (NCOC, *Národní centrum kybernetických operací*), originally provided for by the NCSS as the National Cyber Forces Centre (*Národní centrum kybernetických sil*), has been established within Military Intelligence and is due to become fully operational in 2020. Related legislative amendments have been proposed and await discussion by the Government. Czechia believes that it is essential to have an active cyber defence capacity in the case of some major cyber crisis or disruption. NCOC will therefore be able to conduct a broad spectrum of cyberspace operations and activities

[41] http://www.acr.army.cz/struktura/generalni-stab/sekce-podpory/agentura-komunikacnich-a-informacnich-systemu-86854/ (in Czech).

[42] 'CIRC', http://circ.army.cz/index.html (in Czech).

[43] NCI Agency, 'Malware Information Sharing Platform', http://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf.

[44] http://www.acr.army.cz/informacni-servis/zpravodajstvi/generalni-stab-vybuduje-vysadkovy-pluk--velitelstvi-kybernetickych-sil-a-logistickou-podporu-201395/.

[45] NCSS, p. 18; AP, p. 15-17 (C.9.-C.11.), see n 14 and 15 above.

necessary for ensuring the cyber defence of Czechia, including the support of operations of the Czech Armed Forces in the framework of EU or NATO, or in case of a hybrid conflict.[46] Its competencies and related procedures will derive from a public legal act and classified implementing regulations.

3.5 Engagement with the private sector

Government cooperation with the private sector such as non-governmental CSIRTs, universities, banks and other entities has been taking place on an informal basis, and relations are mostly positive thanks to a long-term building of mutual trust. The Cyber Security Act, which came into force on 1 January 2015, brought some formal obligations for the private sector. For example, ISPs have a duty to report incidents to the National CERT (as opposed to the Government CERT) and, in case of cyber emergency, they have to implement the measures prescribed by the NSA. Private sector operators of CII have yet more obligations (see 0).

The role of the National CERT is performed by the CSIRT.CZ, which is a team operated by CZ.NIC, which is the country code top-level domain trustee and a private law association of ISPs, domain name holders and registrars. The cooperation is based on a public law contract from 18 December 2015 between the NCISA and CZ.NIC. The funding of CSIRT.CZ is provided by CZ.NIC stakeholders, and from research grants and funds; the role of the National CERT is performed free of charge.[47]

The NCISA also has an 'agreement on government security programme' with Microsoft, under which the parties are able to share and exchange cyber security information, which means that the NSA has access to Microsoft products source codes and documentation.[48] A similar information exchange agreement has been concluded with Cisco.[49] Based on this memorandum of understanding, the two entities share cyber threat information and exchange information on current cyber security trends and best practices.

Cooperation between the NCISA and the universities is developing rapidly. The NCSC contributes to cyber security courses, cooperates with university CERT/CSIRTs, and makes use of university cyber infrastructure such as the cyber range of the Masaryk University.[50] Cooperation has also developed in non-technical areas with joint courses on cyber security policies, open source intelligence analysis and related subjects delivered by NCISA at partner universities in Brno, Olomouc and Prague.

Representatives of industry and academia were also closely involved in consultancy capacity during preparations for the amendments to the national regulatory framework in 2017 and 2018. Specific working groups were established to include sectoral authorities, liable entities and expert community to provide comments and suggestions for new legislation.

[46] Concept of the Build-up of the Armed Forces of the Czech Republic 2025, p. 17).

[47] Veřejnoprávní smlouva o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti https://www.csirt.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf (only available in Czech).

[48] 'NSA and Microsoft have signed a crucial agreement on information sharing and exchange', http://www.govcert.cz/en/info/events/nsa-and-microsoft-have-signed-a-crucial-agreement-on-information-sharing-and-exchange/

[49] Národní centrum kybernetické bezpečnosti, 'NBÚ a Cisco uzavřely dohodu o spolupráci v oblasti kybernetické bezpečnosti', http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/nbu-a-cisco-uzavrely-dohodu-o-spolupraci-vnoblasti-kyberneticke-bezpecnosti/.

[50] https://www.kypo.cz/en.

References

Policy

Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020 (2015) http://www.govcert.cz/download/nodeid-590/ (in English).

Akční plán ke strategii pro oblast kybernetické bezpečnosti v České republice na období 2012 – 2015 (2012) http://www.govcert.cz/download/nodeid-896/.

Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020, (2015) http://www.govcert.cz/download/nodeid-973/ (the original Czech version).

Ministry of Defence of the Czech Republic, 'Defence Strategy of the Czech Republic' (2012) http://www.army.cz/assets/en/ministry-of-defence/strategy-and-doctrine/strategie_an.pdf.

Ministry of Defence of the Czech Republic, 'The White Paper on Defence' (2011) http://www.mocr.army.cz/scripts/file.php?id=98276&down=yes.

Ministry of Defence of the Czech Republic, 'The Long Term Perspective for Defence 2030' (2015) http://www.army.cz/images/id_8001_9000/8503/THE_LONG_TERM_PERSPECTIVE_FOR_DEFENCE_2030.pdf.

Ministry of Foreign Affairs of the Czech Republic, 'Security Strategy of the Czech Republic' (2015) http://www.mzv.cz/public/2a/57/16/1375879_1259981_Security_Strategy_CZ_2015.pdf.

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 (2015) http://www.govcert.cz/download/nodeid-1004/ (the original Czech version).

National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020 (2015) http://www.govcert.cz/download/nodeid-1075/ (in English).

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012–2015 (2015) http://www.govcert.cz/download/nodeid-727/.

Strategy of the Czech Republic in the Field of Cybernetic Security for 2012–2015 (2012) http://www.govcert.cz/download/nodeid-1190/.

Cyber Defence Strategy for the years 2018-2022, http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-kyberneticke-obrany.pdf.

Vyhodnocení Strategie pro oblast kybernetické bezpečnosti v České republice na období 2012-2015, (2015) http://www.govcert.cz/download/nodeid-1043/ [Evaluation of the Strategy of the Czech Republic in the field of Cybernetic Security for 2012 – 2015] (only available in Czech).

Zpráva o stavu kybernetické bezpečnosti České republiky 2014 https://www.govcert.cz/download/nodeid-612/ (only available in Czech)

Law

Act No. 300/2008 Coll. on electronic acts and conversion of authorised documents.

Act No. 181/2014 Coll. on Cyber Security and Change of Related Acts (Act on Cyber Security) http://www.govcert.cz/download/nodeid-591/.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ 345/75, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:NOT.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

Nařízení vlády č. 432/2010 Sb. ze dne 22. prosince 2010 o kritériích pro určení prvku kritické infrastruktury
http://portal.gov.cz/app/zakony/download?idBiblio=72819&nr=432~2F2010~20Sb.&ft=pdf.

Usnesení vlády České republiky ze dne 19. října 2011 č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast http://www.govcert.cz/download/nodeid-562/.

Usnesení vlády České republiky ze dne 25. května 2015 č. 390 ke 2. aktualizaci Seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu, https://apps.odok.cz/attachment/-/down/VPRA9X3GH8WY ;

Usnesení vlády České republiky ze dne 1. července 2015 č. 520 o posílení kapacity Národního bezpečnostního úřadu v oblasti kybernetické bezpečnosti v letech 2016 až 2018 https://apps.odok.cz/attachment/-/down/VPRA9Y98PD96 .

Usnesení vlády České republiky ze dne 2. prosince 2015 č. 390 o 3. aktualizaci Seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu, https://apps.odok.cz/attachment/-/down/VPRAA4ZB6POC (only available in Czech).

Veřejnoprávní smlouva o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti, https://www.csirt.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf (only available in Czech).

Vyhláška č. 316/2014 Sb. ze dne 15. prosince 2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) [Regulation No. 316/2014 Coll. of 15 December 2014 on Cyber Security], http://www.nbu.cz/download/nodeid-1067/ .

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)" [Regulation No. 82/2018 Coll. On Cyber Security] https://www.govcert.cz/cs/nova-vkb/.

Vyhláška č. 317/2014 Sb. ze dne 15. prosince 2014 o významných informačních systémech a jejich určujících kritériích [Regulation No. 317/2014 Coll. of 15 December 2014 on Important Information Systems and Their Determining Criteria] http://www.nbu.cz/download/nodeid-1067/ .

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
https://portal.gov.cz/app/zakony/download?idBiblio=82522&nr=181~2F2014~20Sb.&ft=pd f.

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon)
http://portal.gov.cz/app/zakony/download?idBiblio=49557&nr=240~2F2000~20Sb.&ft=pdf .

Other

Agentura komunikačních a informačních systémů, http://www.acr.army.cz/struktura/generalni-stab/sekce-podpory/agentura-komunikacnich-a-informacnich-systemu-86854/

Česká televize, 'Na obranu před kyberútoky dá Česko ročně půl miliardy', http://www.ceskatelevize.cz/ct24/domaci/1532226-na-obranu-pred-kyberutoky-da-cesko-rocne-pul-miliardy

CIRC, http://circ.army.cz/index.html

CSIRT, http://www.csirt.cz/

Datoveschranky.info, 'Datové schránky', 2016 https://www.datoveschranky.info/ .

EU Digital Agenda Scoreboard, 'Digital Economy and Society Index 2015, Country Profile: Czech Republic', https://ec.europa.eu/digital-agenda/en/scoreboard/czech-republic

EU Digital Scoreboeard, Digital Economy and Society Index 2019, Country Profile: Czechia, https://ec.europa.eu/digital-single-market/en/scoreboard/czech-republic

GovCERT.CZ / Národní centrum kybernetické bezpečnosti ČR, http://www.govcert.cz/en/govcertcz/

Masaryk University, 'The KYPO - Cyber Exercise & Research Platform', http://www.kypo.cz/

Ministerstvo obrany České republiky, 'Koncepce výstavby Armády České republiky 2025', 2015 http://www.mocr.army.cz/images/id_40001_50000/46088/KVA___R_ve___ejn____verze.pdf (the original Czech version)

Národní centrum kybernetické bezpečnosti, 'MMR vyhlásilo výzvu na dotace pro zvýšení kybernetické bezpečnosti státních institucí', https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/mmr-vyhlasilo-vyzvu-na-dotace-pro-zvyseni-kyberneticke-bezpecnosti-statnich-instituci/

Národní centrum kybernetické bezpečnosti, 'NBÚ a Cisco uzavřely dohodu o spolupráci v oblasti kybernetické bezpečnosti', http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/nbu-a-cisco-uzavrely-dohodu-o-spolupraci-vnoblasti-kyberneticke-bezpecnosti/

Národní centrum kybernetické bezpečnosti, 'Zkušenosti a výsledky určování KII a VIS', http://www.cybersecurity.cz/data/NBU_2015-KII_VIS.pdf (only available in Czech)

National Cyber and Information Security Agency, www.nukib.cz

National Security Authority http://www.nbu.cz/en/

NATO, 'NATO and Czech Republic bolster cyber defence cooperation', http://www.nato.int/cps/en/natohq/news_123857.htm

NCSC, 'The Government approved first 45 elements of the critical information infrastructure on May 25, 2015' http://www.govcert.cz/en/info/events/the-government-approved-first-45-elements-of-the-critical-information-infrastructure-on-may-25-2015/

NCI Agency, 'Malware Information Sharing Platform' http://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf

'Special Eurobarometer 396 - E-Communications Household Survey', 2013 http://ec.europa.eu/digital-agenda/en/news/special-eurobarometer-396-e-communications-household-survey

Správa základních registrů, 'Roční výpisy o využívání údajů v registru obyvatel a registru osob, Správa základních registrů', 2014 http://www.szrcr.cz/zakladni-registry-dale-zvysuji-transparentnost-verejne

'Studie SPIR - Česká internetová ekonomika', 2013 http://www.studiespir.cz

Studie SPIR – Česká internetová ekonomika, 2016, http://www.studiespir.cz/download/Ceska_internetova_ekonomika_2016.pdf.

Acronyms

AKIS	Agentura komunikačních a informačních systémů - Communication and Information Systems Agency (CISA)
AP	Akční plán – Action Plan
BRS	Bezpečnostní rada státu - State Security Council
CII	Critical information infrastructure – Kritická informační infrastruktura (KII)
CIRC	Computer Incident Response Centre
DNSSEC	Domain Name System Security Extensions
IIS	Important Information System – Významný informační systém (VIS)
ISP	Internet Service Provider
NCKB	Národní centrum kybernetické bezpečnosti – National Cyber Security Centre
NCKO	Národní centrum kybernetických operací – National Cyber Operations Centre (NCOC)
NCSS	National Cyber Security Strategy – Národní strategie kybernetické bezpečnosti
NBÚ	Národní bezpečnostní úřad – National Security Authority (NSA)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost - National Cyber and Information Security Agency (NCISA)
OES	operator of essential services – provozovatel základní služby (PZS)
SME	small and medium enterprise
VKB	Výbor pro kybernetickou bezpečnost – Committee on Cyber Security