CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Tomáš Minárik

# National Cyber Security Organisation: CZECH REPUBLIC

*2nd, revised edition*

Tallinn 2016

*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 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 Slovakia

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

**Upcoming in 2016**

National Cyber Security Organisation in Germany

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)

**Revisions in the 2nd edition:**

- Updated information society indicators;
- Updated to reflect the new Czech National Cyber Security Strategy adopted in February 2015;
- Updates concerning policy coordination in Cyber Security Council (Section 3.1.); conduct of cyber defence exercises (3.2.); active cyber defence (3.3.); critical information infrastructure protection (3.4.1.), and current cooperation with companies and universities (3.5.).

Information in this study was checked for accuracy as of March 2016.

# 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, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the USA as Sponsoring Nations and Austria and Finland as Contributing Participants. 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.

# CZECH REPUBLIC

By Tomáš Minárik
Researcher, NATO CCD COE

## Table of Contents

# 1. Introduction: information society in the Czech Republic

## 1.1. Infrastructure availability and take-up

Basic fixed broadband is available to nearly every Czech household (98% as of 2014).[1] In 2015, 79% of households had some form of internet connection at home, and 77% of the population were regular internet users; 76% of all households and 98% of all enterprises had a broadband connection and there were 28.40 fixed broadband subscriptions per 100 people. A majority (59%) of broadband subscriptions enable download speed of at least 10 Mbps, while 26% enable at least 30 Mbps and 5% allow 100 Mbps (2014).

Mobile broadband coverage reached 97% (Advanced 3G) and 92% (4G) of the population in 2014, while take-up in 2014 was 64.19 subscriptions per 100 people.

All of these figures are close to the EU averages.

## 1.2. E-government and private sector e-services

### 1.2.1. E-government

Despite the legislative framework in place since 2009,[2] the Czech Republic has had mixed success in implementing a comprehensive e-governance agenda. While the availability of e-government services was at 56% for citizens and 100% for enterprises in 2010, the actual use of e-government services had reached only 29% for citizens and 94% for enterprises by 2013, indicating a large gap between the use of e-government services by citizens and by enterprises. This is probably due to the fact that all legal persons were provided with a free but obligatory 'data mailbox'[3] 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 consequently less than 1% have it.[4]

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. So while the Czech Republic ranks as 8th within EU in the use of e-government by enterprises, it is 23rd in the corresponding category for people.

### 1.2.2. E-commerce

The Czech Republic has a relatively high proportion of turnover from e-commerce at 40% for large enterprises (2013) and 26% for Small and Medium Enterprises (SMEs) in 2014. This places it in 2nd place in the EU in both categories. The share of the internet-based economy is estimated at 2.7–3.2% of GDP, and the ICT sector as a

[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] Act No. 300/2008 Coll., on electronic acts and conversion of authorised documents, in effect since 1 July 2009.
[3] Datoveschranky.info, 'Datové Schránky', 2014 <https://www.datoveschranky.info/>.
[4] 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>.

whole produces 4.2% of GDP. The added value for the whole economy from e-commerce, online advertisement and easier access to information is estimated to contribute 8.2–9.5% of GDP.[5]

Some 45% of all individuals order goods or services online (2015), which generally coincides with the EU average (15th place). Cross-border e-commerce is underdeveloped, with only 9% of all individuals ordering goods or services from abroad (25th place).

Overall, the Czech Republic 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 the Czech Republic's enthusiasm for e-commerce into a higher uptake of e-government services by citizens.

# 2. Strategic national cyber security objectives

## 2.1. National cyber security foundation

The Czech Republic's *National Cyber Security Strategy* (NCSS)[6] and the associated *Action Plan* (AP)[7] were drafted by the Czech National Security Authority (NSA)[8] and adopted by the Government in 2015.[9] Both cover the years 2015 to 2020. The previous NCSS and AP covered the years 2012 to 2015.[10]

Cyber security and cyber defence are also mentioned in the *Security Strategy* of the Czech Republic (2015),[11] the *Long Term Perspective for Defence 2030* (2015),[12] the *Concept of the Build-up of the Armed Forces of the Czech Republic 2025* (2015),[13] *Defence Strategy of the Czech Republic* (2012),[14] and in the *White Paper on Defence* (2011).[15]

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

[6] '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).

[7] '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).

[8] National Security Authority <http://www.nbu.cz/en/>.

[9] 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/>.

[10] '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).

[11] 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>.

[12] 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>.

[13] 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> (so far only available in Czech).

[14] 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>.

[15] 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>.

The legal cyber security framework, the *Act on Cyber Security and Change of Related Acts* (Act No. 181/2014 Coll.), was promulgated on 29 August 2014 and took effect on 1 January 2015.[16] The implementing regulations were promulgated on 19 December 2014 and took effect on 1 January 2015.[17]

## 2.2. Cyber security strategy objectives

The previous NCSS (2012-2015), before being replaced by the current NCSS (2015-2020), was evaluated in January 2015 as having achieved most of its objectives.[18] In particular, its two main objectives, of creating the legislative framework of cyber security and establishing the National Cyber Security Centre (NCSC) and Government CERT, were achieved by 2015 (see details in 3.2.). Compared to the previous strategy, which focused on building of basic capacities necessary to guarantee an elementary level of cyber security, the current NCSS (2015-2020) deals with deeper and enhanced modes of cyber security development.

The current NCSS (2015-2020) sets down the visions, principles, challenges, and main goals in cyber security for the Czech Republic. It is worth noting the aspiration of the Czech Republic to 'play a leading role in the cyber security field within its region and in Europe' and 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.'[19] The reference to the protection of the rights pertaining to 'informational self-determination' is also fairly progressive.[20]

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:

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 domestically and internationally. The Czech Republic 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.

---

[16] '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=pdf > (in Czech).
[Act No. 181/2014 Coll. on Cyber Security and Change of Related Acts (Act on Cyber Security)] <http://www.govcert.cz/download/nodeid-591/> (in English).

[17]
- 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;
- Regulation No. 317/2014 Coll. on Important Information Systems and Their Determining Criteria.

All of the above are available in Czech only:
- nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury;
- 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);
- vyhláška č. 317/2014 Sb. ze dne 15. prosince 2014 o významných informačních systémech a jejich určujících kritériích <http://www.nbu.cz/download/nodeid-1067/>.

[18] '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).

[19] NCSS, p. 7.

[20] NCSS, p. 9.

Also, the task of carrying out national cyber security exercises is included under this goal.

***B. Active international cooperation***

This explicitly covers the EU (including ENISA), NATO (including NATO CCD COE), OSCE, UN (including ITU), Visegrad Four countries and the Central European Cyber Security Platform, and bilateral cooperation, including the CERT/CSIRT teams, international organisations and academic centres. The Czech Republic 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)***

The Czech Republic will continue identifying and aiding 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 the Czech Republic. It plans to develop its own capacities and capabilities for cyber security testing, forensic analysis, malware detection and testing, and 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 (NCFC) within the 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 of EU or NATO, or to defend the Czech Republic in a hybrid conflict. Notably, the Czech Republic 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.'
Last but not least, 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 the Czech Republic.

***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 the raising of awareness 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 specialists 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***

The Czech Republic 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, the 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 handle cybercrime cases better.

# 3. National organisational structure for cyber security and cyber defence

## 3.1. Policy coordination and setting strategic priorities

The overall responsibility for national cyber security rests with the Czech **National Security Authority** (NSA)[21] pursuant to Government Resolution no. 781 of 19 October 2011.[22] The same Resolution established the National Cyber Security Centre (NCSC),[23] which is subordinated to the Czech NSA. The NCSC operates the Government CERT; directs cooperation with CSIRTs, both national and international; prepares security standards for various categories of entities in the Czech Republic; supports education and the raising of cyber security awareness; and supports cyber security research and development.

The Government is trying to speed up the development of NCSC by increasing its budget from 2016 and by hiring 24 new staff members in 2016-2018, bringing the total budget up to 115 million CZK[24] and the personnel to 58 in 2018.[25]

Government Resolution no. 781 of 19 October 2011 also established the **Cyber Security Council** (CSC),[26] which is the official forum for interagency coordination.[27] The CSC includes representatives from the Czech NSA, the Ministry of Interior, the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Finance, the

[21] The original name of the NSA in Czech is 'Národní bezpečnostní úřad' (NBÚ).
[22] '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/> (only available in Czech).
[23] The original name of the NCSC in Czech is 'Národní centrum kybernetické bezpečnosti' (NCKB).
[24] About 4.26 million EUR at 27.00 CZK/EUR.
[25] '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> (only available in Czech).
[26] The original name of the CSC in Czech is 'Rada pro kybernetickou bezpečnost' (RKB).
[27] 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).

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 occasionally 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 working group deals with national cyber security issues and the second one covers international issues.

The NCSS Action Plan also assigned several tasks to the Ministry of Education, Youth and Sport; the Ministry of Justice; the Technology Agency of the Czech Republic; and the Ministry of Labour and Social Affairs, even though they are not listed among the bodies represented in the CSC.

The evaluation of the state of cyber security is performed regularly by the CSC members pursuant to the CSC Statute. The annual report on the state of cyber security of the Czech Republic is prepared by the NCSC/NSA, presented to the CSC and approved by the Government.[28] The information on fulfilment of the Action Plan will also be annexed in the annual report from 2016 on.

On 12 October 2015, the Czech Republic, 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.[29]

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

At the operational level there exists the **Government CERT** (GovCERT.CZ)[30] based in Brno, which has 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, which entered into force on 1 January 2015, 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.

These 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, its constituency is public sector and critical information elements of the country's infrastructure (both public and private). Other ISPs continue to report cyber incidents to the national CERT (currently **CSIRT.CZ**),[31] which services the private sector (except the CII).

According to the Act, the Czech NSA may order the listed entities to take further protective measures. The NSA 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.

Together with the Act, the NSA prepared two implementing regulations (No. 316/2014 Coll., Regulation on Cyber Security, and No. 317/2014 Coll., Regulation on Important Information Systems and Their Determining

[28] Compare the 2014 Report on the state of cyber security of the Czech Republic (Zpráva o stavu kybernetické bezpečnosti České republiky 2014) <https://www.govcert.cz/download/nodeid-612/> (only in Czech).
[29] NATO, 'NATO and Czech Republic bolster cyber defence cooperation', <http://www.nato.int/cps/en/natohq/news_123857.htm>.
[30] 'Govcert.CZ / Národní centrum kybernetické bezpečnosti ČR' <http://www.govcert.cz/en/govcertcz/>.
[31] 'CSIRT' <http://www.csirt.cz/>.

Criteria),[32] which provide a detailed description of the preventive security measures listed by the Act. The list is based on the ISO/IEC 27000-series standards and is to include comprehensive management, organisational, procedural and system security elements, with obligations to apply different levels of security measures pertaining to specific categories of entities.

The Regulation on Cyber Security also specifies 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,[33] specified interface, or on paper.

The Czech Republic has taken part in NATO Cyber Coalition exercises since 2010. The agencies involved in 2015 were the NSA, MOD, Ministry of Foreign Affairs, Police, intelligence services, and also the Masaryk University and partners from the private sector (CSIRT.CZ and an antivirus company called AVAST). The Czech Republic also takes part in NATO Crisis Management Exercises (CMX), which usually involve some cyber scenarios. CSIRT.CZ has participated in the Cyber Europe exercises since 2010. National cyber exercises include Cyber Czech, which took place in October 2015[34] and in March 2016, utilising the KYPO Cyber Exercise & Research Platform of the Masaryk University.[35] Last but not least, NSA and CSIRT.CZ take part in regional CECSP Exercises.

## 3.3. Military cyber defence

Military cyber defence is the task of **Communications and Information Systems Agency** (CISA)[36] 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, as well as 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, Allied Rapid Reaction Corps, 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 its 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.'[37] CIRC can prepare remedial countermeasures, tools and procedures, as well as contribute to the awareness of users and managers of CIS, thereby increasing the resilience of CIS and helping to protect data.

[32] n 17.
[33] See part 1.2.1. for the description of data mailbox.
[34] NCSC, 'Cyber Czech 2015 took place on the Cyber polygon in Brno', <http://www.govcert.cz/en/info/events/cyber-czech-2015-took-place-on-the-cyber-polygon-in-brno/>.
[35] Masaryk University, 'The KYPO - Cyber Exercise & Research Platform', <http://www.kypo.cz/>.
[36] 'Agentura komunikačních a informačních systémů' <http://www.acr.army.cz/struktura/generalni-stab/sekce-podpory/agentura-komunikacnich-a-informacnich-systemu-86854/> (in Czech).
[37] 'CIRC' <http://circ.army.cz/index.html> (in Czech).

CIRC also participates in both national and international cyber defence exercises, cooperates with NCIRC, and participates in the Malware Information Sharing Platform.[38]

As regards active cyber defence, it is mentioned abundantly in the NCSS and AP,[39] and the **National Cyber Forces Centre** (NCFC) is being established within the Military Intelligence in 2016 and will be fully operational in 2020. The Czech Republic believes that it is essential to have an active cyber defence capacity in the case of some major cyber crisis or disruption. NCFC will therefore be able to conduct a broad spectrum of cyberspace operations and activities necessary for ensuring the cyber defence of the Czech Republic, including the support of operations of the Czech Armed Forces in the framework of EU or NATO, or in case of a hybrid conflict.[40]

According to information from mid-2015, the Ministry of Defence is expected to be spending 500 million CZK (ca. 18.5 million EUR, about 1% of defence budget) per year on cyber defence in 2016-2020.[41]

## 3.4. Crisis prevention and crisis management

### 3.4.1. Information infrastructure as critical infrastructure

EU Council Directive 2008/114/EC requires that, in order to be considered critical infrastructure, an element or system of infrastructure has to fulfil one of the cross-cutting criteria of significant casualties, economic effects, or public effects. It must also fulfil the sectoral criteria which means that it has to be included on the list of critical infrastructures according to its function.[42] This is codified in Czech law in Act No. 240/2000 Coll.[43] and Government Regulation No. 432/2010 Coll.[44] The list of critical infrastructure, as defined by Czech law, includes communications and information systems in critical sectors such as energy, water management, food industry and agriculture, health service, transport, communication and information systems, financial market and currency, emergency services, and public administration.

According to the Cyber Security Act, CII is defined as 'critical infrastructure falling under the CIS sectoral criterion [pursuant to the Crisis Management Act]'.[45] 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.

[38] NCI Agency, 'Malware Information Sharing Platform' <http://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf>.
[39] NCSS, p. 18; AP, p. 15-17 (C.9.-C.11.), see n 6 and 7 above.
[40] Concept of the Build-up of the Armed Forces of the Czech Republic 2025, p. 17 (n 13).
[41] 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>.
[42] '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> (Gov. Reg. No. 432/2010 Coll., in Czech) § 1.
[43] 'Zákon ze dne 28. června 2000 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> (in Czech), as amended.
[44] Gov. Reg. No. 432/2010 Coll. (n 42). These legal documents reflect the updated European law, namely the 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 L 345/75. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:NOT> In the Directive, critical infrastructure is defined in Article 2 sub (a) as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.'
[45] § 2 sub (b) of the Cyber Security Act. Zákon o kybernetické bezpečnosti (n 16).

On 25 May 2015, the Government of the Czech Republic approved the list of 45 elements of CII operated by ministries and other state organisational units. The list was updated again on 2 December 2015.[46]

As for the non-governmental CII, the process of its determination is ongoing. The elements of non-governmental CII are determined by a 'measure of a general nature' issued by the NSA. By the end of January 2016, 26 companies were included in the list, including electricity, gas and railway companies, air traffic management, mobile operators, major ISPs and banks.

Information systems which are not CII but are nevertheless vital for public administration are termed 'important information systems' (IIS) by the Act on Cyber Security. The IIS operators are subject to only about 60% of the obligations imposed by the Act on Cyber Security, in comparison to CII operators. The list of IIS operated by public authorities contains 92 items,[47] but more IIS fitting the criteria are covered by the cyber security legislation (19 IIS as of September 2015), and an update of the list is being prepared. Also, the distinction between CII and IIS is not fully settled yet, and some IIS may be reclassified as CII.[48]

On 21 September 2015, the Ministry of Regional Development, which is in charge of operational programmes allocating EU structural funds, issued a cyber security call for proposals, specifically aimed at improving the cyber security of CII and IIS.[49] The total funds allocated to this call for proposals are 1 411 764 706 CZK; the applications must be filed between 21 October 2015 and 30 June 2017.[50]

### 3.4.2. Crisis management

The Cyber Security Act introduces the concept of a limited state of emergency known as a 'state of cyber emergency'.[51] 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 NSA for a maximum of 7 days, but can be prolonged repeatedly for up to 30 days.

The Director of the Czech NSA 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, to introduce specific cyber security measures. The state of cyber emergency can be cancelled by the Director of the NSA once the threat has passed. If a threat cannot be managed under the framework of a state of cyber emergency, the Government may declare a general state of emergency.

[46] 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/>;
'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 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).

[47] Compare Annex 1 to the Regulation No. 317/2014 Coll. (n 17).

[48] 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).

[49] 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/>.

[50] About 52.3 million EUR at 27.00 CZK/EUR.

[51] § 21 of the Cyber Security Act. Zákon o kybernetické bezpečnosti (n 16).

## 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 entered 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 Government CERT), and in case of cyber emergency, they have to implement the measures prescribed to them by the NSA. Private sector operators of CII have yet more obligations (see 3.4.1).

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 NSA 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.[52]

The NSA 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.[53] A similar information exchange agreement has been concluded between NSA and Cisco.[54] Based on this memorandum of understanding, these two entities share cyberthreat information and exchange information on current cyber security trends and best practices.

Cooperation between the NSA 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.[55]

[52] 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).
[53] '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/>.
[54] 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/>.
[55] n 35.

# 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, 2012 <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/>.

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 L 345/75. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:NOT> .

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. 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/>.

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=pdf>.

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>.

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 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>.