National Plan for
Research and Development
in Cyber and Information Security
to 2020

TABLE OF CONTENTS

Introduction

The dynamic growth in information and communications technologies has brought about not only new solutions to technical and societal problems, but also new challenges associated with the security of cyberspace in the Czech Republic. The state must therefore be capable of resisting cyber threats that are increasing in both quantity and sophistication[1]. For example, systems utilizing elements of machine learning and artificial intelligence allow large quantities of data to be analysed, and this is leading to increases in sophisticated spear-phishing attacks. The advancing integration of physical devices into computer-controlled systems (Internet of Things) is placing greater demands upon their security, and the same is also true of the advancing digitalization of industrial networks. Cyber security is thus closely connected to research, development and innovation (hereinafter “R&D&I”), which is also reflected in:

- the National Cyber Security Strategy of the Czech Republic for the Period 2015 to 2020 (hereinafter the “National Strategy”)[2];
- the Security Strategy of the Czech Republic[3];
- the National Security Audit from 2016[4];
- the Update of the National Research, Development, and Innovation Policy of the Czech Republic for 2016 to 2020 (2018 update)[5];
- the Inter-Departmental Concept of Support for Security Research in the Czech Republic 2017 to 2023 with an Outlook to 3030[6].

The basic strategic framework for cyber security in the Czech Republic is defined in the National Strategy and in the follow-up Action Plan, approved by Cabinet Resolution No 382 dated 25 May 2015. This resolution imposes upon the National Cyber and Information Security Agency (hereinafter the “NCISA”) an obligation to draw up a National Concept for Research and Development in Cyber Security[7]. However, in view of the dynamics of the evolution of the issue being addressed and the related experience, it was found that science and development requirements in cyber security are better fulfilled by a different type of material – a National

[1] Report on the Status of Cyber Security in the Czech Republic for 2018, available here: https://www.nukib.cz/download/publikace/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

[2] Document available here: https://www.govcert.cz/cs/informacni-servis/strategie-akcni-plan/

[3] Document available here: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

[4] Document available here: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

[5] Document available here: https://www.vyzkum.cz/FrontClanek.aspx?idsekce=866175

[6] Document available here: https://www.mvcr.cz/vyzkum/clanek/koncepce-meziresortni-koncepce-podpory-bezpecnostniho-vyzkumu-cr.aspx

[7] Document available here: https://www.govcert.cz/cs/informacni-servis/strategie-akcni-plan/

Plan which, according to the Methodology for Creating Public Strategies drawn up by the MRD in 2018[8], focuses on dealing with specific objectives and identifying the tools for their achievement. Each chapter also includes analytical bases corresponding to definitions in the conceptual document.

The objective of the presented National Plan is to identify priority research topics pertaining to cyber and information security which are key for the development of the cyberspace security system in the Czech Republic and, at the same time, to set further development objectives, including specific tools that will contribute to the coordination of research activities, cooperation with the private and academic sectors in the development and implementation of technologies, and to the overall development of the research and innovation environment in priority research topics. The National Plan was created in close cooperation with entities from the public, academic and business sectors, with the objective of ensuring the broadest possible consensus as regards the content of the document[9].

The National Plan is valid until 2020. An evaluation of how the objectives under the National Plan are being achieved will be a part of a Notification on the Fulfilment of the Action Plan under the National Cyber Security Strategy of the Czech Republic, which is an annex to the Report on Cyber Security for the preceding period. The evaluation will be conducted on the basis of the performance and evaluation of tasks set out under the Action Plan. Information on the performance of individual measures will also be submitted at a meeting of the Platform for Research and Development in Cyber and Information Security (Chapter 3.2).

[8] Document available here: https://www.mmr.cz/getmedia/08a14dd9-27e8-4a3c-a5cc-532936845297/Metodika-pripravy-verejnych-strategii-zkracena-verze_1.pdf.aspx?ext=.pdf.

[9] In the course of creating the National Plan, the NCISA contacted 16 partners to request their inputs, and several bilateral discussions took place with representatives of the public, academic and private sectors – examples being the Ministry of the Interior, the Office of the Government of the Czech Republic, the Ministry of Regional Development, the Ministry of Industry and Trade, the Ministry of Education, Youth and Sports, and also experts from the Czech Technical University, the Technical University in Brno, and Masaryk University. The National Plan was also discussed within a working group that includes representatives of organizational units of the state focusing on research and development pertaining to cyber security (the Security Information Service, the Office for Foreign Relations and Information, the Czech Police, etc.).

1 NCISA Authority within the System of Support for R&D&I in Cyber Security

The NCISA is the central administrative authority for cyber security in the Czech Republic, and provides for:

- the protection of information and communications systems falling under Act No 181/2014, on cyber security and on changes to related laws (the Cyber Security Act), as amended,
- the protection of information and communications systems falling under Act No 412/2005, on the protection of classified information and on security clearance, as amended,
- cryptographic protection, and
- the publicly regulated Galileo satellite system service.

The NCISA is not a provider of specific and institutional support under Act No 130/2002, on support for research and development from public funds and on changes to certain related laws (the Research and Development Support Act), as amended. However, the Cyber Security Act and the Classified Information Protection Act impose upon it the obligation to perform research and development in cyber security in selected fields of protection of classified information and national cryptographic tools. Thus, in practice, the NCISA functions as both the contracting authority for public contracts for the purposes of the NCISA, and also as the end user of the results of R&D&I.

Further, the NCISA will participate in creating an information and analytical environment for the security community, and will contribute to the coordination of research activities, including the identification of research needs, problems, and priorities in cyber and information security[10]. The role of the NCISA is also to ensure the maximum security and transparency of the technologies used by the state, including testing the security of the technologies being used and their more effective utilization in practice. The activities of the NCISA pertaining to R&D&I are thus not in conflict with the authority of the organizational units of the state providing state aid for R&D&I; rather, the NCISA's activities supplement and develop the said authority.

[10] The NCISA also conducts activities focusing on education pertaining to cyber security in regard to state institutions as well as the public. Information on the research system as well as information obtained from research is also incorporated into educational activities depending on the target audience.

2 Priority Research Topics in Cyber and Information Security

The limited resources available for the support of R&D&I pertaining to cyber and information security must be focused on several key research areas. Therefore, in cooperation with NCISA experts and other professionals from the academic and business sectors, **priority research topics whose stable support is a key requisite for the performance of the NCISA's tasks in view of the current and future needs of the state** have been identified, specifically pertaining to the protection of elements of critical information infrastructure (hereinafter "CII"), significant information systems ("SIS"), basic service operators' systems, critical information infrastructure communications systems[11], and systems handling classified information and cryptography[12].

Initial Situation:

The methods of attack, including their sophistication and force, are also changing as technology develops. According to the Report on Cyber Security in the Czech Republic for 2018, the Czech Republic is facing a significant increase in the numbers of spear-phishing attacks, which attackers utilize to acquire access to a target network. According to the Classification of Incidents Handled in 2018[13], the number of fraudulent incidents utilizing phishing and spear-phishing methods doubled compared to 2016[14].

Another challenge in regard to cyber security is the ability to withstand the exponential increase in the strength of DDoS (distributed denial of service) attacks, the goal of which is to restrict the availability of services. An example is the DDoS attacks on the election process in 2017 and 2018. In 2018, attacks aiming to disrupt the availability of services constituted a total of 33% of all incidents reported to GovCERT. The increasing numbers of attacks involving advanced social engineering imposes significant demands on the ability of the state to protect its networks and other elements of CII and SIS. The increasing digitalization of industrial networks and SCADA systems means we can anticipate increased pressure for research and development into tools that will be able to better protect communications and information networks. Examples of such tools are the automation of penetration testing and advanced network operations monitoring, including data collection for forensic analysis.

In connection with the increasing numbers of IoT devices, the growth in technologies improving connectivity (5G networks), and the continuously growing utilization of cloud

[11] Act No 181/2014, on cyber security.
[12] Act No 412/2005, on the protection of classified information and on security clearance.
[13] Report on Cyber Security in the Czech Republic for 2018.
[14] Report on Cyber Security in the Czech Republic for 2016.

infrastructure capacities, there is also increased potential for the use (and abuse) of applications utilizing elements of artificial intelligence. It is therefore necessary to focus efforts on research and development into tools to analyse large volumes of data and automate solutions to cyber security incidents.

Research topics pertaining to cryptographic protection and the development of cryptographic tools are based upon the internal needs of the NCISA in providing for cryptographic protection, as well as upon consultations with experts in the fields in question. These are topics focusing, for example, on the development of special measuring methods and technologies to provide protection from compromising electromagnetic emissions, and research and development into cryptographic algorithms resistant to breaches, for example, through post-quantum cryptography research.

2.1 Priority Research Topics Pertaining to Protection of Elements of CII, SIS and Basic Service Operators' Systems:

- Advanced penetration testing methods and automation,
- analysis of network communications and the development of unique detection techniques in network operations using advanced security information management and threat intelligence,
- new methods of protection against DDoS attacks,
- security of industrial networks and SCADA/ICS systems in connection with the growth of IoT and connections to the cloud,
- development of technologies and methods to increase protection from privacy breaches and identity theft,
- protection from sophisticated forms of spear-phishing,
- research and development into artificial intelligence algorithms to strengthen cyber security and state strategic networks and systems resilience,
- forensic investigation – development of tools for working with electronic evidence,
- development of post-quantum cryptography methods able to resist quantum attacks,
- protection from sophisticated forms of malware,
- support for the development of a cyber security certification and standards system,
- security policy, future trends in cyber security legislation, creation of crisis scenarios and methodologies pertaining to cyber security,
- development of tools for simulation and technical exercises in cyber security,
- application of a distributed decentralized database (blockchain) in cyber security.

2.2 Priority Research Topics Pertaining to Protection of Classified Information and Communications Systems:

- Development pertaining to the interconnection of information systems with varying information security requirements,
- development pertaining to the secure utilization of virtual tools in information systems,
- development pertaining to issues defined within NSA Security Standard 1/2012 on Re-Use, Reduction and Termination of Classification Level in Modern Information Mediums,
- development of new methods ensuring adequate protection of classified information at Confidential or higher classification level against its possible disclosure through compromising emissions.

2.3 Priority Research Topics Pertaining to Cryptographic Protection and Development of Cryptographic Tools:

- Development and analysis of nationally unique cryptographic algorithms (primitives, diagrams, and protocols) for the protection of classified information,
- adaptation and examination of options to utilize international cryptographic algorithms from the NATO and EU environments (primitives, diagrams, and protocols), and interoperable protocols for the protection of classified information,
- development and certification of cryptographic tools for the protection of classified information and critical infrastructure information,
- testing and analysis of publicly issued cryptographic algorithms and their implementation,
- preparation of cryptographic protection from quantum threats – analyses of the security and appropriateness of using various countermeasures and quantum-resistant algorithms,
- high-speed data encryption and hardware acceleration of cryptographic tools,
- research and development into cryptographic data authenticity protection in the IoT and sensor network environments,
- evaluation of threats and risks, and creation of crisis scenarios and methodologies relating to cryptographic protection,
- technologies ensuring secure access to the publicly regulated Galileo satellite system service signal.

3 R&D&I Development Objectives in Cyber and Information Security

This chapter identifies five development objectives and specific tools to achieve them. The purpose of the objectives set out below is to contribute to the development of the research and innovation environment in priority research topics pertaining to cyber and information security. The achievement of the individual objectives will be covered from the existing NCISA research and development budget. Nevertheless, it is advisable for there to be a gradual increase in funds so that it will be possible to conduct, for example, research missions abroad under the NCISA budget (see Objective 5).

Table: List of Objectives

Objective 1 – Priority research topics will be a part of public tenders and calls in national and international programmes supporting research, development, and innovation
Objective 2 – Greater involvement of the user community in R&D&I support systems in cyber security, including reinforcement of the ability to put results into practice
Objective 3 – The NCISA as an R&D&I information and analytical environment in cyber security
Objective 4 – Advanced international cooperation
Objective 5 – The NCISA as an active participant in jointly conducted research and development in cyber security at EU level

3.1 Objective 1 – Priority Research Topics Will Be a Part of Public Tenders and Calls in National and International Programmes in Support of Research, Development, and Innovation

Initial Situation:

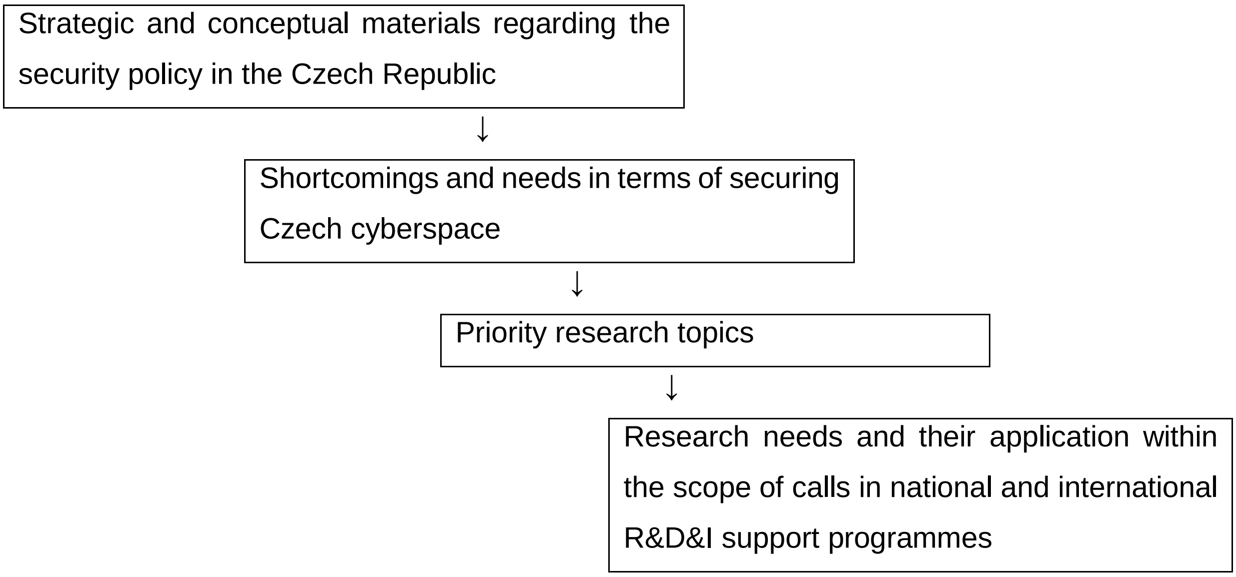
The NCISA has not yet had a comprehensive and publicly accessible list of research topics to be promoted with regard to the public administration authorities, the academic community, and the private sector with the goal of ensuring their stable support and sufficient funding at national and international levels[15].

[15] The research topics are also in accordance with the strategic cyber security priorities of the European Network and Information Security Agency (ENISA), see Analysis of the European R&D Priorities in Cybersecurity, European Cyber Security Organization – SRIA.

Tools:

- The NCISA will create a list of research needs/objectives based on priority research topics, including a definition of the research objective and a description of the required results. The list will reflect shortcomings and needs in terms of securing Czech cyberspace, including current security trends (see the diagram). The priority research topics will be promoted primarily within the scope of R&D&I support programmes under the responsibility of:
  - The Ministry of the Interior of the Czech Republic – Czech Republic Security Research Programme for 2015 to 2022, Security Research Programme for the Needs of the State 2016–2021, and Strategic Support for the Advancement of Security Research in the Czech Republic 2019–2025 (IMPAKT 1),
  - the Technology Agency of the Czech Republic – BETA2 programme,
  - the Ministry of Regional Development – Integrated Regional Operational Programme for 2021–2027[16],
  - the Ministry of Industry and Trade – TREND and The Country for the Future programmes,
  - and other programmes overlapping into cyber and information security.

Diagram: System for the Identification of Research Needs



Strategic and conceptual materials regarding the security policy in the Czech Republic

↓

Shortcomings and needs in terms of securing Czech cyberspace

↓

Priority research topics

↓

Research needs and their application within the scope of calls in national and international R&D&I support programmes

[16] The NCISA will seek the re-announcement of the "Cyber Security" call, which was announced in 2015 within the scope of the 2014–2020 programme period.

3.2 Objective 2 – Greater Involvement of the User Community in R&D&I Support Systems in Cyber Security, Including Strengthening the Ability to Put Results into Practice

Initial Situation:

The NCISA participates in the implementation of several projects and, depending on their focus, acts as project sponsor, public contract contracting authority, or end user responsible for putting new technologies into practice. At the same time, the NCISA also closely cooperates with state aid beneficiaries, as well as with specialized units of the Czech Police and intelligence services concerned with cybercrime. These entities have knowledge of practical needs and are thus able to assess project proposals in terms of their societal relevance. It is therefore necessary to emphasise more intense involvement of the user community at various decision-making levels of the R&D&I support system in cyber security.

Tools:

- The NCISA will initiate and support the involvement of the user community in:
  - the boards of programmes of the Ministry of Interior of the Czech Republic and of other providers of state aid for R&D&I,
  - databases of examiners at the MI, TACR, and MIT,
  - inspection activity during project implementation,
  - the relevant bodies of the Horizon 2020, Horizon Europe, and Digital Europe programmes,
  - national and international programme initiatives.
- Regular analysis and collection of information on the current needs of end users through a newly created Platform for Research and Development in Cyber and Information Security, the main tasks of which will be to:
  - ensure synergies between the research capabilities of the academic community and the needs of end users working in cyber security,
  - monitor the demands placed upon the application of products on the market,
  - seek mutual topics of interest and prevent overlaps in research,
  - mediate the transmission of R&D&I results to potential producers and end users,
  - evaluate the status of national and international cooperation in regard to R&D&I,
  - evaluate the current technological trends in cyber security, and ensure mutual sharing of information among the individual entities involved.
- The NCISA will support the creation of Digital Innovation Hubs and other platforms where research results are transferred into practice.

3.3 Objective 3 – NCISA as an R&D&I Information and Analytical Environment in Cyber Security

Initial Situation:

There are currently a number of information tools providing information on national and international research programmes. However, the information is not concentrated in a single information source, topic-wise it does not focus exclusively on the issue of cyber security, and thus does not fully serve experts in cyber security. It is therefore desirable to create an information source on the NCISA website where one can find information on EU framework programmes, current programme calls pertaining to cyber security, or guidance on participation in international consortiums. The development of the information environment will also involve the monitoring and analysis of current trends in cyber and information security with the goal of providing partners with interesting information on new technologies and security calls.

Tools:

- Create and regularly update a "research" tab on the NCISA website,
- the NCISA will send out a newsletter to partners six times per year with up-to-date information on cyber security R&D&I, which it will also place on the website,
- a NCISA representative will, if financially possible, take part in networking events organized by the European Commission and other EU bodies in an effort to facilitate participation by Czech entities in international consortiums under the European research programme Horizon 2020, respectively Horizon Europe and Digital Europe, or the Internal Security Fund (ISF) and the Connecting Europe Facility (CEF),
- the NCISA will prepare a list of national and international contact details, using which it will contact partners with an offer to participate in relevant research projects,
- each month, the NCISA will send partners a monitoring report regarding open resources focusing on technological trends falling within the priority research topics,
- the NCISA will create a comprehensive Report on Trends in Cyber and Information Security, the outputs of which may, inter alia, be utilized as a basis for the further focusing of R&D&I support and setting current priority research topics. The Report will be created using the NCISA's own resources.

3.4 Objective 4 – Advanced International Cooperation

Initial Situation:

Cross-border cooperation brings not only access to foreign know-how, but also opens up the way to diversification of financing sources for research activities. In the Czech Republic, there are a number of top research institutions and companies for which international research cooperation is a normal part of their operations. However, the success rate of the involvement of Czech entities in projects financed through European research programmes is still low[17]. The NCISA is able to help in this regard by creating the conditions for the development of contacts with leading foreign institutions and, at the same time, by supporting the research community through its own participation in international projects.

Tools:

- The NCISA will support the creation of international consortiums and, with regard to the internal capacities of the NCISA, will become involved in international projects, the results of which have the potential to contribute to improving the protection of Czech cyberspace,
- in cooperation with cyber-attachés, science diplomats and embassies abroad, the NCISA will organize research missions abroad with the goal of engaging in long-term strategic cooperation with major institutions abroad. In the course of preparing the topical focus of the missions, the NCISA will cooperate with the MI and the MD to focus support into priority cyber security research topics,
- the NCISA will continue to ensure support for the performance of obligations arising from international treaties and from the membership of the Czech Republic in expert groups and organizations of an international nature operating in cyber and information security R&D&I,
- the NCISA will actively participate in jointly conducted research and development in cyber and information security at NATO level.

[17] Frank, D., Albrecht, V. (2016): Participation of the Czech Republic in H2020 and in the Euratom programme January 2014 – May 2017, ECHO, 2016, Annex 3-4/2016, 34 p.

3.5 Objective 5 – NCISA as an Active Participant in Jointly Conducted Research and Development in Cyber Security at EU Level

Initial Situation:

There are currently intensive negotiations under way at EU Member State level regarding the form of framework programmes in connection with the preparation of a new programme period for 2021–2027. The EU is also increasing its capacity pertaining to the protection of Member States from increasingly frequent cyber threats, and has commenced the preparation of a new structure for the consolidation and creation of networks of its expert knowledge in various areas of cyber security. Due to the national position of the NCISA in cyber security, it is natural that the NCISA will play an active role in the formation of new EU framework programmes and, in cooperation with other agencies, will support national initiatives focusing on an active role for the Czech Republic in improving the resilience of the EU to cyber threats.

Tools:

- The NCISA will promote priority research topics under the Horizon Europe and Digital Europe programme calls,
- support for the creation of a National Coordination Centre in the Czech Republic in connection with a proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[18],
- the NCISA will support the creation of a European Centre for Excellence in AI in the Czech Republic, which will, among other things, focus on the cyber security of AI products, services, and processes, as well as on preventing the misuse of AI technologies,
- the NCISA will strengthen cooperation with other foreign organizations with an impact on the focus of research and development at EU level (e.g., the European Cyber Security Organization – ECSO, and the European Network and Information Security Agency – ENISA),
- the NCISA will cooperate with other government administration authorities within the scope of the EU Cohesion Policy,

[18] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

- the NCISA will strengthen cooperation with the Horizon 2020 programme board delegate (or that of Horizon Europe), national contact points, and liaison officers for research, development, and innovation in Brussels.

4 Risk Management – Limitations and Conditions

A key precondition for the achievement of a majority of the objectives set out above is adequate staffing of the NCISA. A lack of qualified personnel may lead to a suppression of certain activities, primarily in international cooperation or the creation of an information environment. Further, it is necessary to at least maintain the existing level of funds allocated to research and development and other auxiliary activities. In the short and medium terms, it is desirable to increase funds that will be utilized, for example, to provide for the participation of a NCISA staff member at project team meetings abroad (in the event of the participation of the NCISA in an international project), or in the implementation of research missions abroad. In there is a lack of funds, research missions abroad will need to be carried out in cooperation with other agencies, such as the MI, the MD or the MFA.

Further, it is necessary to set up cooperation with other agencies in an appropriate manner and to continue to deepen such cooperation. The successful implementation of certain measures is dependent upon joint action and, in the event of failure thereof, there is a danger of major shortcomings in the implementation of specific measures.

A further external limitation is the periodicity of state aid programmes and the relevant calls being announced. If allocated funds are used up, there may not be new calls announced in 2020, which would significantly limit the capability to implement the measures under Objectives 1 and 2.

An analogous situation may also occur in terms of the structure and implementation of new EU programmes or the manner in which the conditions for applicants for financial support are set. In this regard, the NCISA has limited options as to how to prevent such risks. Two of these are active participation by the NCISA in creating R&D&I priorities in the Czech Republic and abroad, and close cooperation with the entities responsible for individual research programmes.

5 Outlook to 2023

After this National Plan comes to an end, i.e. after 2020, it may be assumed there will be an evaluation of the experience from the new procedures that this plan is putting in place. An evaluation will be made of the ability of the NCISA to fulfil the set objectives, as well as whether the priority research areas are still current in view of the dynamics of cyber threat trends. Cyber and information security R&D&I will also be impacted by the set-up of the new programme period 2021–2027 and by the trends in R&D&I support from national funds. The subsequent National Plan for the period 2021–2022 will be drawn up in close connection with the Cyber Security Strategy of the Czech Republic for 2021 to 2025.

6 Objective Achievement Plan

OBJECTIVE	TOOL	INDICATOR	TO BE EXECUTED BY	IN COOPERATION WITH	TO BE CONSULTED WITH	TO BE ACHIEVED BY
1	Drawing up a list of research needs/objectives, including a definition of the research objective and a description of the required results. The list will reflect the shortcomings and needs in securing Czech cyberspace, including current security trends	List of research needs/objectives	NCISA	Czech Police, Security Information Service, Military Intelligence, Office for Foreign Relations, and Information	MI, MD, MEYS, MIT, TACR, MRD, RDIC	2020
		Increasing number of projects implemented with a focus on priority research topics compared to the previous year				2020
2	Involvement of the user community in: • the boards of programmes of the Ministry of Interior of the Czech Republic and of other providers of state aid for R&D&I, • databases of examiners of the MI, TACR and MIT,	Increasing number of experts engaged		Czech Police, Security Information Service, Military Intelligence, Office for Foreign Relations and Information, and	MI, MD, MEYS, MIT, TACR, MRD, RDIC	2020
		Creation and twice yearly meeting of a Platform for Research and Development in Cyber and				2019-2020

	- inspection activity in the implementation of projects, - the relevant bodies of the Horizon 2020, Horizon Europe and Digital Europe programmes, - national and international programme initiatives Regular analysis and collection of information on the current needs of end users by way of a newly created Platform for Research and Development in Cyber and Information Security The NCISA will support the creation of Digital Innovation Hubs and other platforms where research results are transferred into practice.	Information Security	NCISA	other external partners		
				Academic and private sectors	MIT, MEYS, MRD	2020

3	Create and regularly update a “research” tab on the NCISA website	Creation of the tab on the site	NCISA	TCCAS		continuous
	Create a newsletter with news about cyber security R&D&I	Newsletter 6x per year with R&D&I news				2019–2020
	Participation in networking events organized by the European Commission			TCCAS	Academic and private sectors	2019–2020
	The NCISA will prepare a list of national and international contact details, on the basis of which it will contact partners with an offer to participate in relevant research projects	Continually updated list of national and international contacts				continuous
	Each month, the NCISA will send partners a monitoring report regarding open resources focusing on technological trends falling within the priority research topics	Monitoring report of open resources 12x per year				2019–2020
	The NCISA will create a comprehensive Report on	Report on Trends in Cyber and				2020

	Trends in Cyber and Information Security, the outputs of which may, *inter alia*, be utilized as a basis for further focusing of R&D&I support and setting current priority research topics.	Information Security 1x per year			Academic and private sectors	
4	The NCISA will support the creation of international consortiums and, depending on the internal capacities of the NCISA, will become involved in international projects, the results of which have the potential to contribute to improving the protection of Czech cyberspace	Increasing number of project applications submitted jointly with a foreign partner	NCISA	Academic and private sectors, TCCAS	Czech Police, Security Information Service, Military Intelligence, Office for Foreign Relations and Information, and other external partners	continuous
	Implementation of research missions abroad	Research mission 2x per year, including subsequent evaluation of the benefits of the missions		MI, MD, MFA		2020

	Support for the performance of obligations arising from international treaties				MFA	continuous
	The NCISA will actively participate in jointly conducted research and development in cyber and information security at NATO level			MD, Military Intelligence		continuous
5	Promote priority research topics under Horizon 2020, Horizon Europe, and Digital Europe programme calls	Priority research topics as a part of the Horizon Europe and Digital Europe programmes	NCISA	MEYS, OGCR, MIT	Czech Police, Security Information Service, Military Intelligence, Office for Foreign Relations and Information, academic and private sectors	2020
	Support for the creation of a National Coordination Centre in the Czech Republic in connection with a proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research	Creation of a National Coordination Centre	NCISA	OGCR, MEYS, MF, MIT		2020–2021

	Competence Centre and the Network of National Coordination Centres					
	Support the creation of a European Centre for Excellence in AI in the Czech Republic		NCISA	MIT, OGCR, MEYS, MT		2020–2021
	Strengthen cooperation with other foreign organizations that have an impact on the focus of research and development at EU level		NCISA	Academic and private sectors, TCCAS		continuous
	Cooperate with other government administration authorities within the scope of the EU Cohesion Policy		NCISA	MRD, MI		continuous
	Cooperate closely with the Horizon 2020 programme board delegate, or that of Horizon Europe		NCISA	MEYS		continuous

7 List of Abbreviations

CEF – Connecting Europe Facility

ECSO – European Cyber Security Organization

ENISA – European Network and Information Security Agency

EU – European Union

ISF – Internal Security Fund

CII – Critical Information Infrastructure

MT – Ministry of Transport

MRD – Ministry of Regional Development

MD – Ministry of Defence

MIT – Ministry of Industry and Trade

MEYS – Ministry of Education, Youth and Sports

MI – Ministry of the Interior

MFA – Ministry of Foreign Affairs

NATO – North Atlantic Treaty Organization

NSA – National Security Authority

NCISA - National Cyber and Information Security Agency

RDIC – Research, Development, and Innovation Council

TACR – Technology Agency of the Czech Republic

TCCAS – Technology Centre of the CAS

OGCR - Office of the Government of the Czech Republic

R&D&I – Research, development, and innovation

SIS – Significant information systems