NATIONAL CYBER SECURITY STRATEGY CZECHIA

NÚKIB

National Cyber
and Information
Security Agency

Table of contents

Introduction by the Director of NÚKIB

The National Cyber Security Strategy you are now reading builds on the solid foundations of more than fifteen years of tradition in the strategic development of a secure cyberspace in Czechia at both national and international level. We are currently witnessing fundamental changes in the international security environment, with cyber threats taking on new forms and their actors becoming more ambitious.

Our time is marked by constant pressure to digitise all areas of life, which poses the challenge of ensuring the stability, protection and sustainable development of information technology and society itself. Many of these technologies are now an essential part of the state's functioning, the economy and our everyday communication as citizens. At the same time, we are witnessing a growing dependence on these technologies, accompanied by a heightened risk of their misuse for cyberattacks. The scale and intensity of cyberattacks have surged in recent years, and their potential is certainly far from exhausted. It is therefore necessary to place more emphasis than ever on strengthening defence capabilities, employing modern security technologies and deepening cooperation among the public, private, and academic sectors.

This strategy builds on key national and international strategic documents that define the core security orientation of Czechia and reaffirm its strong anchoring in the European Union (EU) and North Atlantic Treaty Organization (NATO). These include, for example, the Security Strategy and Defence Strategy of the Czech Republic, both adopted in 2023, the 2020 EU Cybersecurity Strategy for the Digital Decade and the 2022 NATO Strategic Concept. Experience gained through the preparation and implementation of previous national cyber security strategies, which provided us with valuable insights into the functioning of the cyber security system in Czechia, also played an important role in shaping this document. Alongside the necessary analysis of the current security environment and the definition of objectives for the years ahead, the strategy also includes a realistic assessment of Czechia's current internal capabilities and identifies areas in need of further development. Beyond the technical dimension, we must also increasingly address societal issues, such as the effective implementation of the legal framework and the advancement of international cooperation.

Ing. Lukáš Kintr

Director of National Cyber and Information Security Agency

I am convinced that the successful implementation of a strategic vision in a field as broad as cyber security depends above all on an interdisciplinary approach and synergy among all stakeholders. Together, we must foster an environment in who security is an integral part of every decision – whether it relates to deploying new technologies, adopting legislation, training professionals, or sharing information in our personal lives. Investment in cyber security – and especially in those who provide it for us – is not only a necessity, but also a competitive advantage that supports our country's economic growth.

Czechia is well positioned to counter new threats successfully, and I believe that this strategy will serve as a long-term foundation not only to strengthen our defence and security in both the digital and physical domains, but also for promoting Czechia's prosperity and social cohesion.

National Cyber and Information Security Agency

This National Cyber Security Strategy (NCSS) was prepared by the National Cyber and Information Security Agency (NÚKIB) and was approved by the Government of the Czech Republic in September 2025 with effect from 2026, replacing the previous strategy from 2021.

List of Abbreviations Used

5G	5th Generation Mobile Networks
6G	6th Generation Mobile Networks
AČR	Armed Forces of the Czech Republic
APT	Advanced Persistent Threat
BIS	Security Information Service
CERT	Computer Emergency Response Team
PRC	People's Republic of China
CIWC	Cyber and Information Warfate Command
ČTÚ	Czech Telecommunication Office
EDTs	Emerging and Disruptive Technologies
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IoT	Internet of Things
IP4	Indo-Pacific Four (informal designation for Australia, New Zealand, Japan and the Republic of Korea as NATO's Indo-Pacific partners)
ITU	International Telecommunication Union
MoD	Ministry of Defence
MIT	Ministry of Industry and Trade
MEYS	Ministry of Education, Youth and Sports
MoI	Ministry of the Interior
MFA	Ministry of Foreign Affairs
NATO	North Atlantic Treaty Organization
NBÚ	National Security Authority
NCKO	National Cyber Operations Centre

NCSS	National Cyber Security Strategy
NÚKIB	National Cyber and Information Security Agency
OSCE	Organisation for Security and Cooperation in Europe
OECD	Organisation for Economic Cooperation and Development
UN	United Nations
PCR	Police of the Czech Republic
PPP	Public Private Partnership
RF	Russian Federation
ÚZSI	Office for Foreign Relations and Information
VZ	Military Intelligence

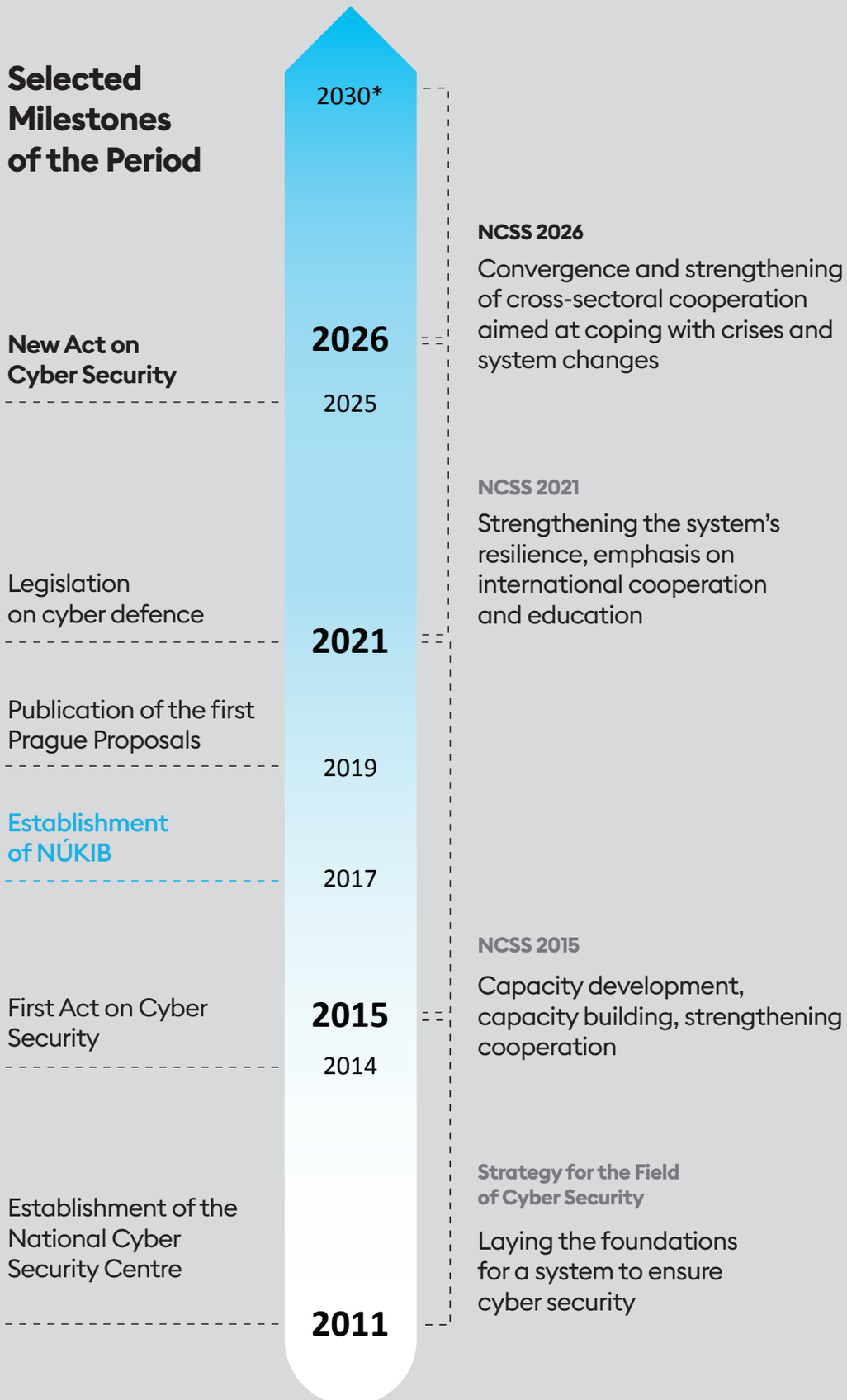
Summary of the Strategy

The NCSS is Czechia's highest-level national strategic document on cyber security and an integral part of Czechia's strategic framework. It establishes a coherent and coordinated framework focused on:

- **the security and resilience of information and communication systems;**
- **cyber defence;**
- **cyber diplomacy; and**
- **combating cybercrime and strengthening societal resilience against threats in cyberspace.**

The NCSS is divided into an analytical and a strategic section. The analytical section describes the current security environment and the state of cyber security in Czechia. It is based on a SWOT analysis, which examines external factors (threats and opportunities in the environment) and internal factors (strengths and weaknesses of Czechia's cyber security system). Based on these findings, the subsequent strategic section formulates a vision and sets strategic objectives for its implementation. The NCSS is based on the Methodology for the Preparation of Public Strategies issued by the Ministry of Regional Development.

Development of Czechia's Strategic Direction in Cyberspace



*According to the law, the NCSS shall be updated at least once every five years; an earlier update is possible.

Analysis of the Current Situation

External Factors:
Security Environment

Threats

The international security environment is deteriorating and becoming less stable, which is also reflected in cyberspace.

The number and capabilities of attackers are increasing. Czechia is primarily targeted by state-sponsored groups and cybercrime actors.

The global expansion and professionalisation of cybercrime continue. In terms of total damages, it currently matches the world's strongest economies.

Growing dependence on both conventional and new technologies, as well as their suppliers, is increasing vulnerabilities.

Personal and other sensitive data are being disseminated uncontrollably and processed in countries with varying levels of security.

Opportunities

Deepening national and international cooperation in ensuring cyber security and defence can help compensate for the lack of resources and capabilities.

Intensified cooperation among the private, academic and public sectors strengthens the ability to manage crises in cyberspace.

New technologies can increase the effectiveness of the fight against cyber threats.

In addition to enhancing protection, investment in cyber security can also deliver competitive market advantages and act as a driver of economic growth.

In addition to private and public organisations' own resources, funding for cyber security can also be sourced from EU projects and grant programmes.

Internal Factors: Czechia's Cyber Security System

Weaknesses

Staffing and funding for cyber security are insufficient in both the public and private sectors.

There are significant disparities in the level of security culture and security itself across regulated entities and within society at large.

Funding conditions and regulations, especially those from the EU, are unclear and continue to grow in complexity.

A reactive approach still prevails in state security institutions, and some processes are either inadequately defined or unnecessarily complex.

Strengths

Czechia has built an advanced system for ensuring its cyber security.

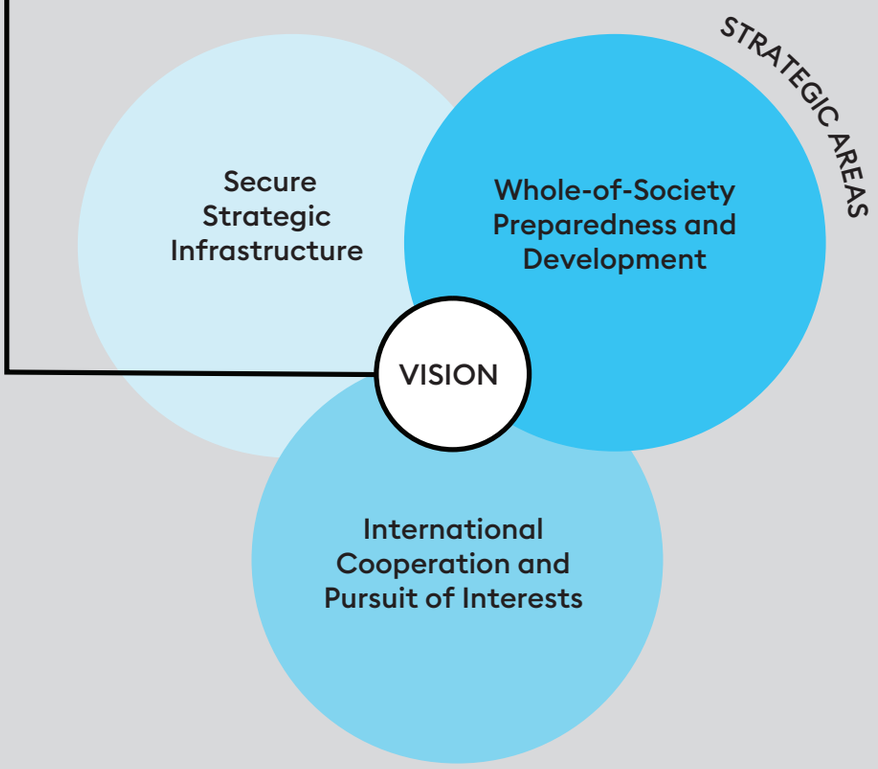
Czech institutions and experts possess a high level of expertise and enjoy a strong reputation internationally.

A well-functioning security community exists across the private, academic and public sectors.

The Czech private and academic sectors have strong innovation potential.

Vision and Strategic Objectives

Czechia will be a secure and digitally advanced country with resilient information infrastructure, an educated, critically thinking, and innovative society, and strong international and domestic partnerships through which it will ensure the effective protection and promotion of its interests in cyberspace.



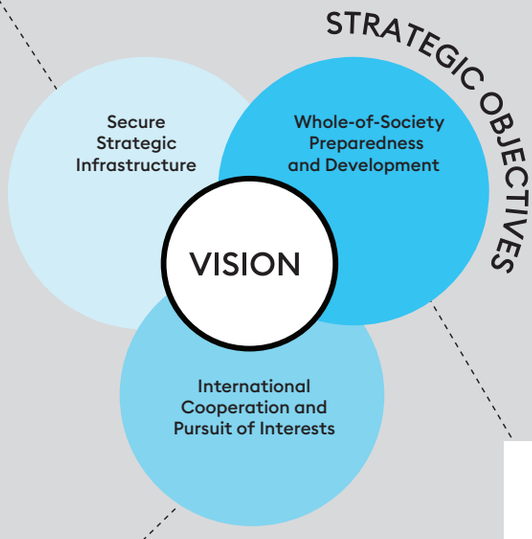
"Effectively managed and resilient infrastructure, free of risky dependencies, that proactively protects organisations and individuals from threats in cyberspace."

"Confident international engagement by Czechia and building trustworthy partnerships to secure a strong global standing and a leading role in the region."

"An educated society with a strong pool of experts, mutual cooperation and support for innovation as a prerequisite for long-term sustainable security."

STRATEGIC OBJECTIVES

- Protection and Resilience of Strategic Infrastructure against Anticipated and Unanticipated Threats
- Proactive Approach, Effective Detection and Efficient Response to Cyber Attacks and Crises, including Cyber Defence and Fight against Cybercrime
- Regulation Balancing National Security and Individual Rights
- Strengthening Financing and More Efficient Use of Resources in the Public Sector
- Unifying Public IT Architecture and Strengthening Data Governance with an Emphasis on Security
- Promoting Secure and Resilient Supplies beyond Strategic Infrastructure



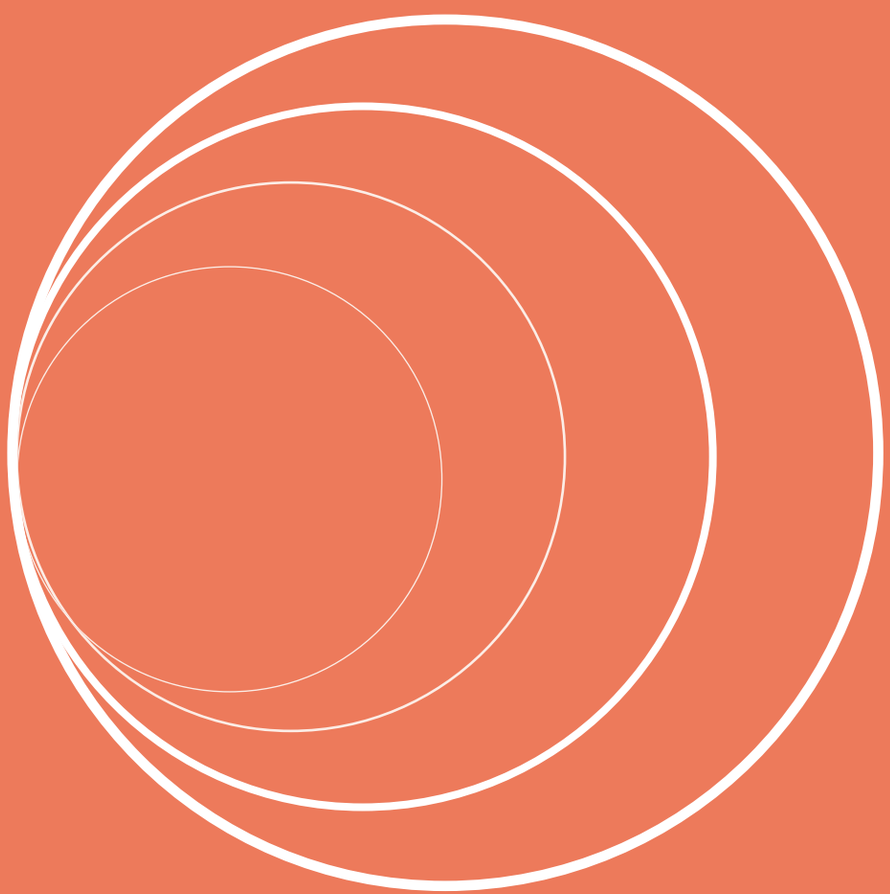
STRATEGIC OBJECTIVES

- Establishing New and Strengthening Existing Strategically Important Partnerships
- Active Promotion of Czechia's Interests, Objectives and Priorities in Shaping International Rules and the EU Law
- Assertive Action against Hostile Acts by Malicious Actors in Cyberspace, including Attribution of Attacks, Diplomatic Response and Imposing of Sanctions
- Promoting Open Strategic Autonomy
- Protecting Global, Open, Secure and Free Cyberspace
- Strengthening International Information Sharing and Development Cooperation

STRATEGIC OBJECTIVES

- Strengthening Numbers and Motivation of Experts for the Long-term Sustainability of Czechia's High Level of Cyber Security
- Development of Whole-of-Society Digital Competences and Cyber Security Culture
- Enhanced Cooperation to Coordinate and Overcome Differences Across Sectors
- Developing the Knowledge and Skills of Cyber Security Experts
- Supporting Research and Innovation in Cyber Security
- Promoting the Emergence of Secure Technological Alternatives

External Factors: Security Environment



The international security situation is deteriorating, and the existing security architecture is being shaken. We are witnessing a global power struggle and a transformation of the international order, with some states redefining their international interests and the way they pursue them. There is a risk of escalation of ongoing armed conflicts, and the outbreak of new ones cannot be ruled out. Cyberspace has become a standard battleground in contemporary international conflicts. Dynamic technological developments bring new opportunities, as well as threats, while the existing ones remained unresolved.

The dependence of states and societies on information and communication technologies (ICT) continues to grow, increasing the significance of vulnerabilities in these technologies and their potential exploitation by malicious actors. Attackers' capabilities are expanding, and both the number of cyberattacks and the range of their potential targets are steadily growing. Cybersecurity is therefore assuming ever greater importance as one of the fundamental prerequisites for the functioning of the state's economy and the protection of individuals' rights.

A New Geopolitics of Cyberspace Is Taking Shape

The international security situation has undergone profound changes in recent years. The free and open Internet, based on a multistakeholder governance model, has long been under attack by certain states that seek to restrain and fragment this model and to bring the Internet under their control. Cyber operations taking place not only in the context of the war in Ukraine and the Israeli-Palestinian conflicts confirm that cyberspace has become a standard arena for contemporary conflicts and that it is undergoing a process of so-called weaponisation. It is being exploited for military purposes, hybrid operations and the preparation of potential operational environments for possible engagement in the event of armed conflict. This trend will undoubtedly continue and will also affect Czechia. Even in a situation where there is merely the threat of an armed conflict involving NATO Allies, intense cyberattacks on both military and civilian infrastructure can be expected. This holds valid even if Czechia were to serve solely as a transit and host country for Allied units and equipment.

Access to data, technology, production capacity, raw materials and other resources is and will remain critical. The growing influence of multinational corporations at the expense of nation states is becoming increasingly evident. **The challenge for Czechia, the EU and NATO is to achieve open strategic autonomy: a balance between self-sufficiency and economic openness to the outside world. This is made particularly difficult by the shortage of secure and competitive domestic technological alternatives, which deepens dependence on the technologies of foreign rivals.**

OPPORTUNITY

Most states, including Czechia, lack sufficient opportunities and capacities to secure all the necessary resources and technologies themselves. For resource-constrained states, the solution to this situation lies in intensive **cooperation with reliable partners, both at the supranational and international levels. Cooperation in this respect is crucial, especially within NATO and the EU, as well as in the OSCE, OECD, ITU, the Council of Europe and the United Nations (UN). At the national level, it cuts across the individual components of government, industry, and civil society.**

A proven model for strengthening and enhancing cooperation is, for example, purpose-built public-private partnerships (PPP) and deepening cooperation with national and international partners on research and development projects.

Supporting the development and production of security solutions within Czechia, the EU and NATO has the potential not only to strengthen the cyber resilience of all participating countries, but also to contribute to their economic growth and prosperity. Joint coordination and harmonisation of regulations and public policies also contribute to a uniform and generally higher security standard and can reduce the transaction costs of cross-border trade.

Threat Actors

The main actors threatening the cyber security of Czechia and the wider democratic world are states that conduct state-of-the-art cyber operations with political objectives. These activities are primarily used to advance strategic interests, weaken counterparts and obtain valuable intelligence.

Russian Federation (RF): A Long-term and Immediate Threat to Czechia's Security

The RF is the biggest direct and long-term threat not only to Europe's cyber security, but also beyond. Its strategy combines cyberattacks with hybrid operations to weaken states' defense capabilities, undermine trust in democratic institutions and destabilise both society and the economy.

The RF has been aggressive towards Czechia and its allies in cyberspace, with activities including cyber espionage, sabotage and influence operations. It primarily targets strategic government institutions, but also private businesses and individuals who oppose Russian interests or support Ukraine. The attack conducted by the RF against Czech institutions via vulnerabilities in Microsoft Outlook application was also the first case of public attribution of a cyberattack by Czechia. It occurred in May 2024.

The RF's aggressive policy, the war in Ukraine and the threat of a conflict between the RF and a NATO Ally will remain a key source of threats for Czechia in the future. At the same time, it can be expected that if peace is concluded in Ukraine, the RF will reallocate its freed capacities towards further malicious activities in cyberspace and preparations for the next armed conflict.

People's Republic of China (PRC): A Sophisticated Actor with Global Ambitions

The PRC poses a complex systemic challenge to democratic states. It seeks to reshape the international order to its advantage, employing a combination of cyber operations, socio-economic coercion, and hybrid actions. Its cyber operations are primarily focused on espionage and gaining access to critical systems, with the aim of controlling or exploiting them at an opportune moment (a practice known as prepositioning). The targets include government institutions, the academic sector, telecommunication and sectors of high strategic value. The PRC's cyber espionage attack on the Czech Ministry of Foreign Affairs (MFA) was the second instance of public attribution by Czechia carried out in May 2025.

Czechia is also threatened by the high level of Chinese technologies present in its strategic infrastructure. Given the Chinese legal environment and the unconditional obligation of Chinese companies to cooperate with the regime, this increases the threat of espionage, sabotage, and technological dependence. It can be expected that the PRC's expansive policy, including the growing tensions in the Indo-Pacific region and especially around Taiwan, will remain a source of threats to Czechia's economic and technological security in the years ahead.

Other State Actors

In cyberspace, Czechia also faces threats from:

Democratic People's Republic of Korea, which perpetrates financially motivated cybercrime to fund its nuclear programme, circumvents sanctions and conducts cyber espionage targeting strategically important technologies, including weapons research and satellite systems.

Islamic Republic of Iran, which generally carries out cyberattacks against Western states, Israel and Arab countries in the Persian Gulf; in Czechia, Iran's malicious activity has been detected in connection with critical infrastructure in the water management sector.

In view of the very dynamic trends in the international security environment, it cannot be ruled out that, in the coming years, other states will join the ranks of those posing threats to Czechia in cyberspace.

These states generally operate in cyberspace through highly sophisticated so-called Advanced Persistent Threat (APT) groups, whose members are linked to the intelligence services or armed forces the states concerned. However, such groups are not always directly under government control and may also pursue their own cybercrime or hacktivist objectives. APT groups conduct long-term, sophisticated, targeted operations and strive for a long-term covert presence in compromised systems. The most significant threat to Czechia is posed by APT groups linked to the RF and the PRC.

Cybercrime groups are also significantly malicious actors for Czechia. Their main motivation is to generate an economic benefit. In some cases, these have evolved from informal criminal gangs into ostensibly legitimate business entities that commercially develop and sell malicious tools (**cybercrime as a service**) or conceal their criminal or other harmful activities behind legitimate activities.

Highly sophisticated tools for conducting this criminal activity, including artificial intelligence technologies, which were previously accessible only to economically powerful state actors or entities sponsored by them, are now cheaper and easily available even to less capable attackers. This trend is expected to continue, with the number of cyberattacks and attackers, as well as the damage caused by cybercrime, continuing to rise.

Despite the declining anonymity of the online environment, law enforcement authorities' efforts to combat and prevent cybercrime are hampered by the growing use of anonymisation tools and services. However, the ongoing discussion about the possibility of the across-the-board disruption of such tools and services by law enforcement authorities encounters concern over the creation of new vulnerabilities and their potential exploitation by malicious actors, which could result in a compromise of all electronic communication content.

In 2023, the global damage caused by cybercrime reached EUR 7.81 trillion – comparable to the world's third largest economy in terms of the volume of funds. By 2030, the global damage caused by cybercrime is expected to rise to EUR 28.22 trillion, roughly triple the 2023 amount. **Global revenues from cybercrime are projected to surpass those from the illegal drug trade by 2025**[1]**.**

In 2023 alone, Czech banks registered nearly 70,000 victims of cybercrime among their clients, with their total losses amounting to EUR 55.22 billion. **Compared to 2022, the number of incidents recorded by banks in Czechia tripled, while some victims are believed not to have reported the attacks at all**[2]**.**

In terms of the impact of their activities, **hacktivist groups** that use cyberspace for political, social or other activism, and in some cases also have ties to state actors, are for now less significant, yet still relevant threat actors for Czechia.

Many of these state and non-state actors cooperate or coordinate their activities on either a short- or long-term basis, which further amplifies the threats they pose.

Technological Advances are Accelerating Changes in the Cyber Environment

Owning to technological progress, continued digitalisation and geopolitical tensions, cyberattacks are now more sophisticated and more accessible than ever before, and attackers are actively exploiting this. **According to the analysis by Check Point Software Technologies, in the third quarter of 2024 the average number of cyberattacks per company in Czechia increased by 69 %**[3].

Emerging and Disruptive Technologies (EDTs) are fundamentally changing the way both the digital and physical worlds operate. Artificial intelligence, quantum computing, the Internet of Things, autonomous transport and military systems, cloud technologies and certain new-generation electronic communications network technologies (e.g. 5G and 6G) are accelerating the pace at which society, the economy and the functioning of the government and security are transforming. EDTs bring new opportunities for efficiency and performance, but they also increase energy consumption, reduce the transparency of IT systems, and create scope for new cyber threats and vulnerabilities.

OPPORTUNITY

Along with new threats, the need to find new security solutions is also increasing. EDTs, particularly **artificial intelligence and post-quantum cryptography, offer more effective and advanced means of strengthening cyber security and defending not only** against new, but also existing threats. As in other fields of human activity, the introduction and operation of cyber security tools based on new technologies can also bring significant reductions in total security costs.

In addition to the emergence of new technologies, new ways of using existing ones also play an important role for the security of Czechia and its partners. One example is satellite services, which, in addition to navigation, are increasingly used to transmit data and encryption keys, thereby reducing dependence on terrestrial infrastructure, but also creating more avenues for compromising the security of transmitted information.

Increasing Complexity and Volume of Data in Cyberspace

The trend towards the increasing quantity and complexity of ICT and ICT systems, as well as their growing interconnectedness, continues. These systems are becoming increasingly demanding in terms of management, security and effective threat monitoring. **The consequences of cyberattacks or unintentional technical errors can be more severe for society than ever.** Even a minor breach in the security of a single system can cause widespread disruption to the drinking water supplies, train operations, healthcare delivery or fuel production and distribution. Assigning low priority to cyber security within an organisation, or investing in untrusted and insufficiently secured technologies, can therefore result in substantial economic losses, the misuse of sensitive data, or even a direct threat to human health and life.

OPPORTUNITY

Individuals' and organisations' interest in cyber security is increasing, as are the economic opportunities in this field. Although investments in cyber security represent a financial burden for both private and public budgets, these **investments pay off in the long run. For organisations, the cost of implementing security measures is almost invariably many times lower than the expense of addressing the damage caused by a successful cyberattack.** For example, according to a report4 by the European Union Agency for Cybersecurity (ENISA), organisations that invested in modern security tools, including artificial intelligence and automation, saw an average reduction in the data breach cost of EUR 1.57 million and shortened the time needed to identify and resolve a cyber incident by 108 days.

At the national and societal level, well-targeted investments in cyber security constitute a strategic contribution to know-how, technological development and Czechia's competitive advantage.

Effective use of available external financial resources, such as EU subsidy programmes, also represents an opportunity to further develop and strengthen cyber security.

Global supply chains are vulnerable and can be disrupted or compromised. Dependence on foreign technology suppliers increases the risk of Czechia's strategic dependence on other states and limits its ability to deal with crises. Entire industries often rely on individual suppliers due to their market dominance or the absence of suitable alternatives. In the public sector in particular, the replacement of a supplier is further complicated by disadvantageous contractual terms, which can effectively bind an organisation's operations to the existing supplier – a situation known as vendor lock-in.

Individuals and organisations share large volumes of data about themselves in cyberspace, including personal and other sensitive data. Such data, shared both intentionally and knowingly, as well as unintentionally or even completely unknowingly, **then become assets to the companies whose services process and sell them on, and from which both private and public entities can derive an unprecedented amount of information.** This trend is particularly driven by the widespread use of mobile and IoT devices, as well as the digitalisation of public services and records. Data are also frequently stored outside the EU or outside countries with comparable protection standard, significantly increasing the risk of data theft or misuse. The growing use of digital identities and the digitalisation of financial transactions, combined with advanced social engineering techniques, also facilitates the perpetration of **financial fraud.**

In the second half of 2023 and the first half of 2024, ENISA[4] recorded **over 11,000 cyber incidents in the EU**, many of which occurred in public infrastructure and private companies. The average cost was estimated at over EUR 3.97 million.
Below are selected examples of attacks and vulnerabilities with a significant impact on public infrastructure:

The attack on the **Irish Health Service (2021),** which necessitated the forced shutdown of all its information systems, forced many hospitals to postpone scheduled surgeries and examinations. The ransom demanded was **EUR 19 million**, but the government refused to pay. The total damage was estimated at up to **EUR 613.65 million**, and full restoration of the systems took over three months.

An attack by a Russian-speaking cybercrime gang on **Costa Rica's** information systems **(2022)** paralysed the operation of 27 government institutions for several weeks and threatened the country's financial system. The hackers demanded a ransom of **EUR 17.59 million,** which the government refused to pay. The total damage to the private sector alone was estimated at almost **EUR 122.7 million** within the first 48 hours of the attack.

A ransomware attack on a UK health service subcontractor **NHS Advanced (2023)** caused outages in more than two hundred hospitals and clinics. Although the ransom amount paid was not disclosed, the damage was estimated at **tens to hundreds of millions of euros.**

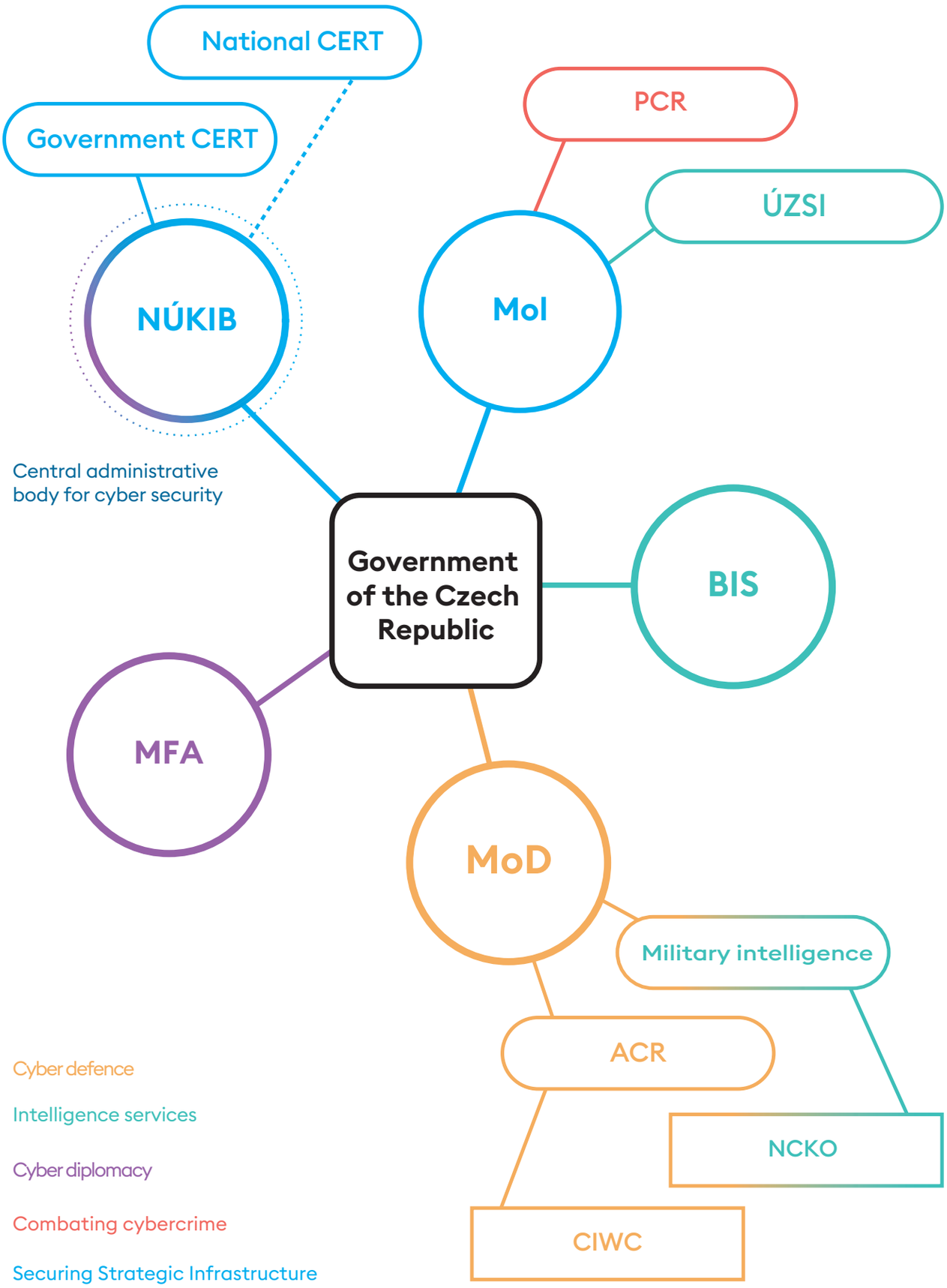
An error in a security tool update from the company **Crowdstrike (2024)** caused a global outage of Windows on approximately **8.5 million installations**, including systems in the financial sector, public administration, aviation and emergency services. Although this was not a deliberate attack, but rather an unintentional vulnerability in the supply chain, the costs resulting from the reduction of services were estimated at over **EUR 9 billion.**

Internal Factors: Cyber Security System in Czechia

Czechia has a well-developed system for ensuring cyber security with a strong position of NÚKIB and other state institutions, which also includes the private, academic and non-profit sectors. Cyber security has become an important component of Czechia's national security. Despite all the progress, further strengthening of resilience and responsiveness to increasingly sophisticated threats are hindered in particular by a shortage of funding, skilled experts, and alternative technological solutions, as well as by the uneven level of security among regulated entities.

Over the fifteen years of continuous strategic planning, cyber security in Czechia has evolved from a technical discipline confined to individual organisations to a society-wide, multidisciplinary issue and a key element of national security. Building on the foundations already laid, capacities for cyber defence continue to be developed, efforts to combat cybercrime are being intensified, and cyber diplomacy is being expanded.

Role of Key Institutions in Czechia's Cyber Security



Alongside NÚKIB, as the central administrative authority for cyber security, the system for safeguarding Czechia's cyberspace also includes the entities responsible for specific key areas (see diagram above). In line with the whole-of-government approach, the system involves numerous other state authorities that, within their areas of competence, make a significant contribution to secure cyberspace, such as the Ministry of Industry and Trade, the Czech Telecommunication Office and the Ministry of Education, Youth and Sports. The Governmental CERT and National CSIRT hold a special role in coordinating national-level monitoring, detection, and response to cyber security incidents. NÚKIB and other state institutions have gradually established themselves as respected and trusted authorities in these areas, both domestically and internationally.

In addition to the state's regulatory, supervisory and coordinating role, non-state actors also contribute to ensuring cyber security in Czechia. Together, the public and private sectors form Czechia's strategic infrastructure. The overall level of its security depends on the security standard of individual regulated entities and their ability to cooperate and share information.

Regulated entities

Regulated entities, in the context of the NCSS, are public and private organisations and individuals whose rights and duties derive from legal regulations governing any of the areas of cyber security. Examples of such legal regulations include the Act on Cyber Security, the Act on Electronic Communications and the General Data Protection Regulation (GDPR).

Strategic infrastructure

Strategic infrastructure refers to equipment, resources and other components of systems that are strategically important for ensuring the functioning of the state and society. In the field of cyber security, strategic infrastructure mainly includes the information and communication systems of the state and other regulated entities.

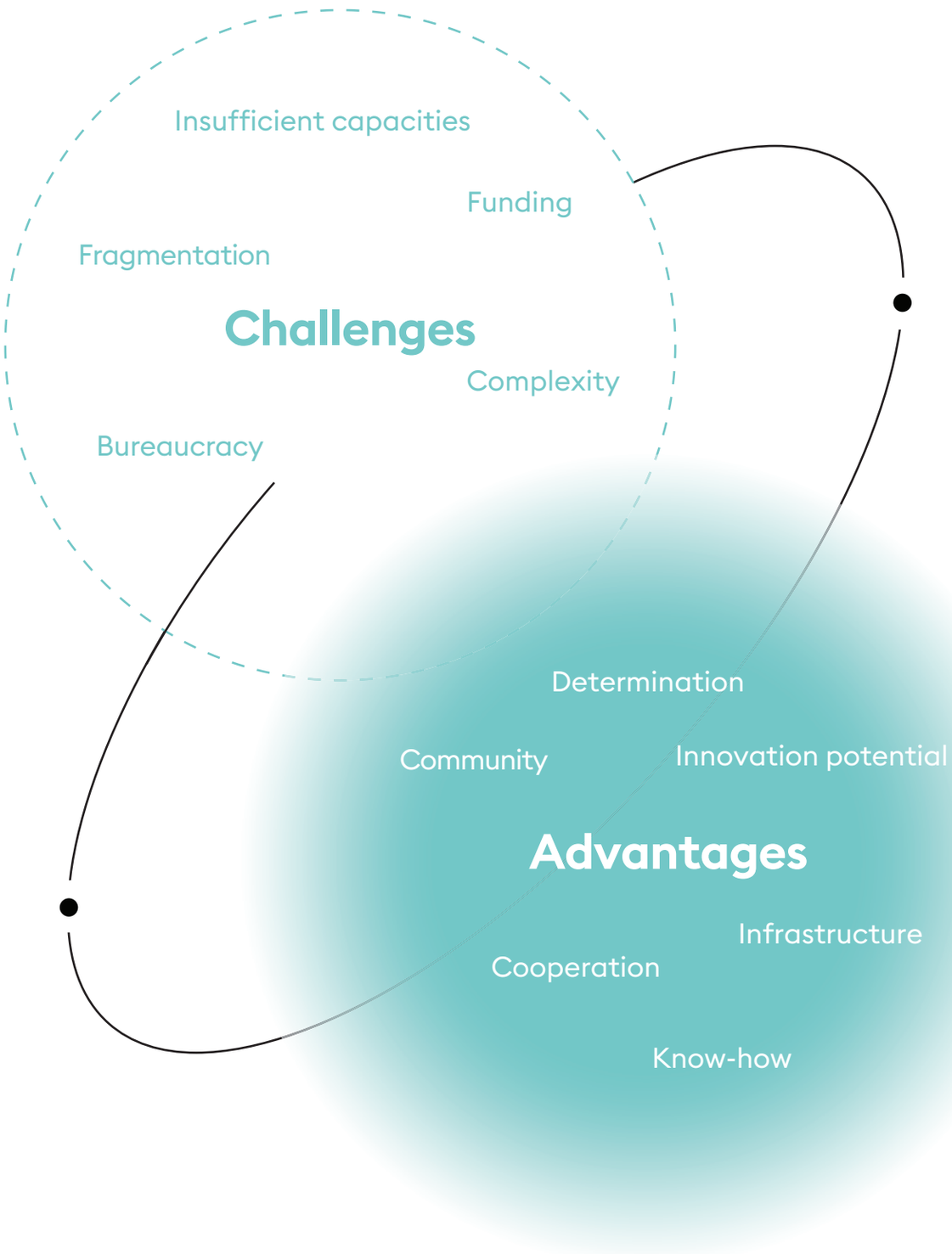
Czechia has long been among the world's pioneers in the protection of strategic infrastructure in cyberspace and in the exercise of public administration in this field. In 2014, it became one of the first countries in the world to adopt a comprehensive cyber security act, based on contemporary legal doctrine and industry standards. Czechia is active in preparing and implementing EU and NATO legislation and policies, and it develops its own security mechanisms, such as security screening of strategic infrastructure supply chains. Many countries in Europe and beyond began building their cyber security capacities and legal frameworks much later, and the expertise of Czech specialists, both technical and non-technical, has long been a highly sought-after and valued export of the Czech diplomacy.

Czechia also has a well-functioning community of cyber security experts from various specialisations across state and non-state institutions. This community enjoys the trust of private and academic stakeholders and, together with them, serves as a source of innovation and a carrier of unique know-how. **The high qualifications of Czech experts and their innovative potential are further demonstrated by the fact that some of the most widely used commercial ICT security tools are developed by Czech companies or have domestic origins.** NÚKIB's role as the national coordinator in cyber security research and development is emphasised as it supports the participation of Czech industry and academics in cross-border projects and facilitates their access to grant funding.

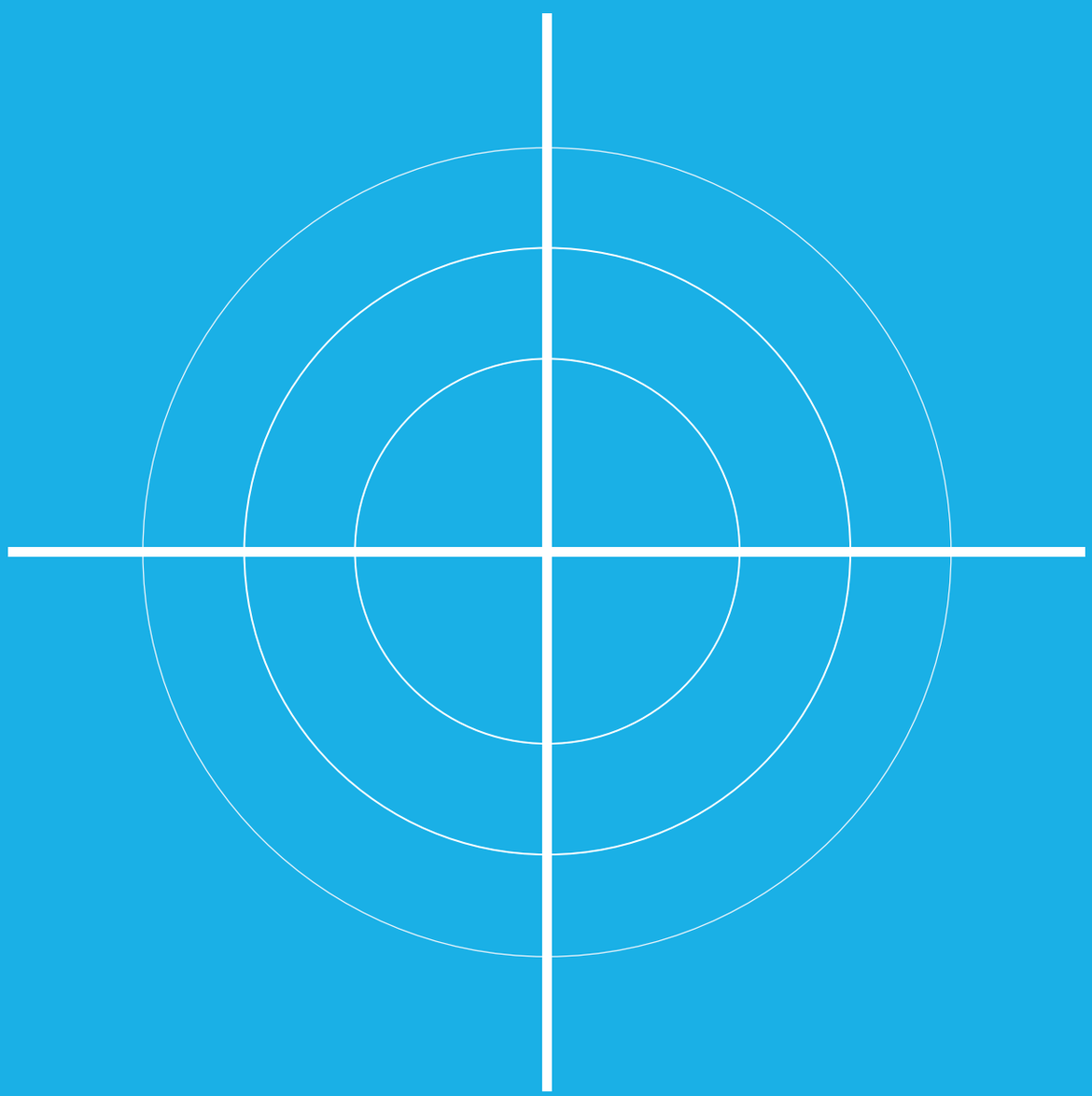
Despite these strengths, ensuring cyber security in Czechia faces certain limitations and shortcomings. **The most significant and persistent challenge for Czechia's cyber security is the shortage of expert personnel and the way the funding system is set up.** The shortage of experts - up to 300 0005 in the EU as whole - affects small and medium-sized enterprises and public administration in Czechia. The continued deterioration of this state of affairs, especially in the public sector, stems from insufficient allocations from the state budget for expert salaries and rigidly set remuneration rules. Resources allocated to cyber security-related capital and operational expenditures in both the public and private sectors, although gradually increasing, are still insufficient. Procedural barriers also prevent many organisations from drawing sufficient funds from national or EU funding sources and the practical use and deployment of research results is often problematic.

The shortage of personnel and funding has far-reaching negative consequences for infrastructure security and economic performance. As shown not only by NÚKIB's Cyber Security Status Reports6, the lack of resources already undermines the ability to withstand increasingly sophisticated cyber threats and to respond flexibly to the rising number of cyber security incidents.

Czechia's cyber security is also adversely affected by the uneven security maturity of regulated entities and the growing complexity and fragmentation of the regulatory environment. This is due, among other factors, to the sharp increase of the EU legislation with an impact on cyber security in recent years and to the differing security requirements of sectoral regulations. System resilience and responsiveness are also negatively affected by complex or missing processes – for example, for sharing sensitive but unclassified information or for coordinated response to large-scale crises. Yet, the proper setup of these processes is essential for Czechia's ability to manage crises, defend itself in the event of involvement in an armed conflict, and to meet the NATO commitments.

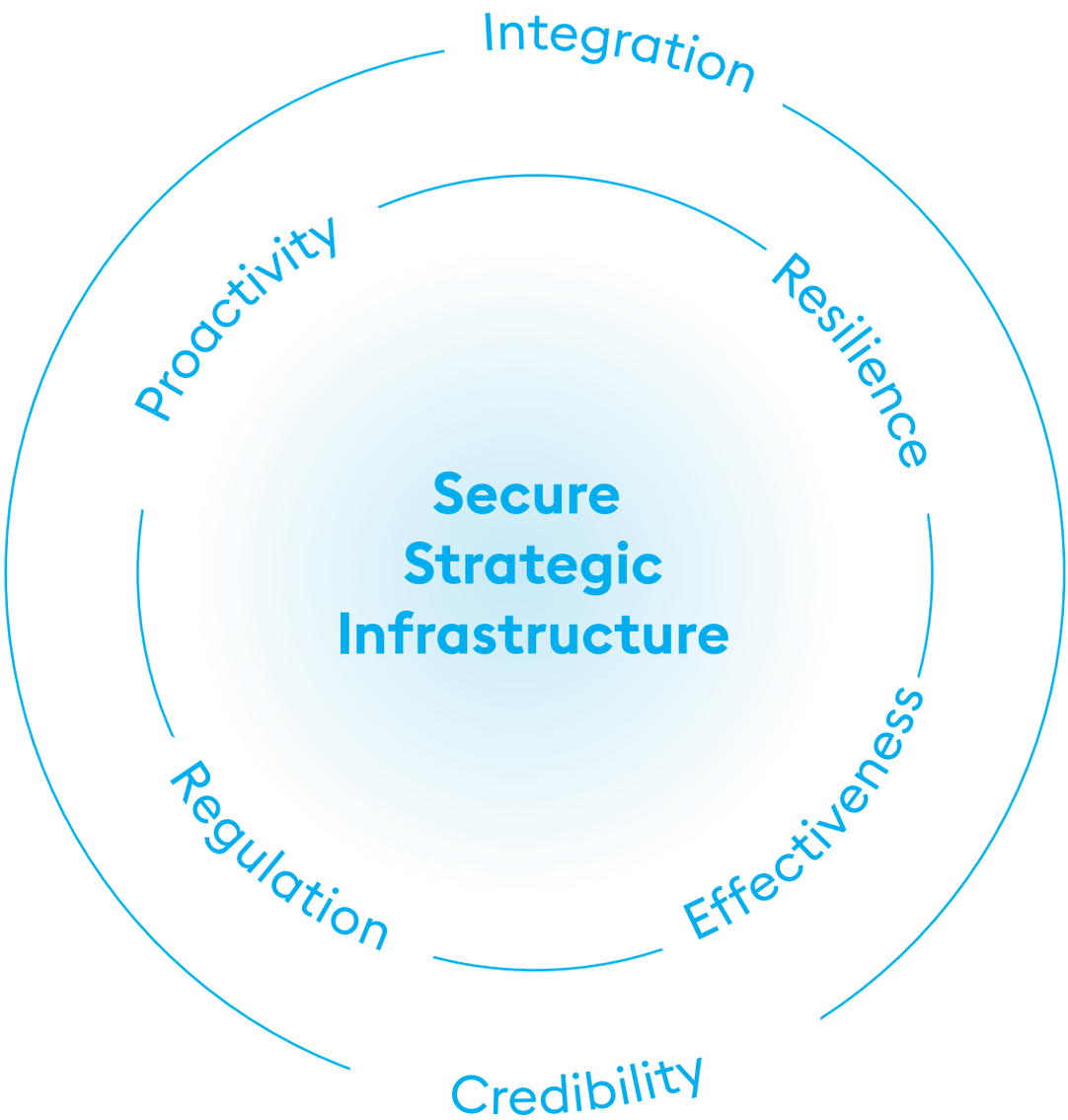

Insufficient capacities
Funding
Fragmentation
Challenges
Complexity
Bureaucracy
Determination
Community
Innovation potential
Advantages
Infrastructure
Cooperation
Know-how

Vision and Strategic Objectives



Vision

Czechia will be a secure and digitally advanced state with resilient information infrastructure, an educated, critically thinking, and innovative society, and strong international and domestic partnerships through which it will ensure the effective protection and promotion of its interests in cyberspace.


Integration
Resilience
Effectiveness
Credibility
Regulation
Proactivity
Secure
Strategic
Infrastructure

Strategic Area: Secure Strategic Infrastructure

Czechia will strengthen its resources and develop its capabilities for proactive and effective responses to cyber threats, including building its own cyber defence capabilities. A stable legal framework and effective public administration will ensure a secure and reliable environment for organisations and individuals. The strategic infrastructure will be prepared to face current and future challenges, thereby supporting Czechia's stability, development, and security in cyberspace.

Protection and Resilience of Strategic Infrastructure Against Anticipated and Unanticipated Threats

The protection and resilience of strategic infrastructure against a wide range of threats from cyberspace and the physical environment, including hybrid threats, will be continuously strengthened in order to minimise the risks arising from them. Emphasis will be placed on ensuring the high security and reliability of both new and existing ICT products through regular audits, updates and vulnerability testing.

The security of strategic infrastructure essential for the functioning of the state will be at the level of the current state of knowledge in this area and will make use of EDTs, including protection against threats arising from these very technologies. In view of progress in quantum computing, a transition to post-quantum cryptography will be ensured to safeguard the confidentiality of data against decryption in a post-quantum world. Artificial intelligence tools will be employed to detect and protect against attacks conducted using such technologies.

In cases where attacks cannot be prevented, the priority will be to ensure continuity or timely restoration of service provision with minimal impact on the state, organisations and individuals. Infrastructure resilience will focus not only on protecting national systems (at both nationwide and regional levels) and the services they provide, but also on meeting Czechia's Alliance commitments.

Proactive Approach, Effective Detection and Efficient Response to Cyberattacks and Crises, including Cyber Defence and Fight against Cybercrime

Capabilities for effective detection and rapid and effective response to cyberattacks will be developed both on the part of state authorities with competences in the field of cyber security, defence and combating cybercrime, and within other strategic infrastructure.

Through active monitoring and analysis of current and potential threats in cyberspace, including proactive scanning for hidden threats and indicators of compromise, the effective detection of security events and incidents will be ensured. This will enable rapid and effective responses to prevent or mitigate their impacts.

Czechia will strengthen its capacity to effectively detect, investigate and counter cybercrime. Tools will be developed for the rapid detection and analysis of criminal activities in cyberspace, as well as legal, technological, and other mechanisms enabling effective prosecution of offenders without lowering cyber security standards or unduly infringing individuals' privacy. In the fight against cybercrime, Czechia will also focus on prevention and awareness-raising and will support victims of cybercrime.

Czechia will respond to cyberattacks assertively, in political, economic, diplomatic, and criminal-law terms, so that attackers do not profit from harmful activities in the long term and they desist from them. Where appropriate, Czechia will coordinate its response with partners, especially within NATO, and its response may include the use of passive or active cyber defence. For these purposes, offensive and multi-domain capabilities will continue to be developed to ensure Czechia's security and defence. Countering cyber threats through cyber defence will be defined by a legal framework that enables effective actions both in peacetime and in the event of a transition to crisis. To this end, cooperation across public and private strategic infrastructure actors will also be strengthened, including integrating capabilities, sharing information, organising joint exercises, and making use of non-state capabilities to address crises.

Regulation Balancing National Security and Individual Rights

The legislative framework and public policies in cyber security will be as clear, professionally understandable, future-proof and technology neutral as possible, following the example of current good practice. A balance will be maintained between the interests of society and those of the individuals affected. Emphasis will be placed on consolidation and unification of regulatory requirements.

Regulation will enable both its creators and addressees to respond flexibly, yet predictably, to security and technological developments, in order to create a safe and fair competitive environment and to promote efficiency and innovation. State authorities will have the necessary tools and powers to protect the non-distributive rights of citizens, while being monitored to ensure that the effectiveness of such powers is not compromised.

New cyber security legislation and policies will be drafted with an emphasis on coherence with the overall regulatory framework and the ability of the addressees to implement and comply with them in the long term. In this respect, Czechia will actively support the addressees of regulation and provide them with high-quality methodological guidance, while at the same thoroughly monitoring and enforcing compliance with the established rules.

Strengthening Financing and More Efficient Use of Resources in the Public Sector

The public administration will systematically plan and allocate investment and operational resources for cyber security according to the real needs of the organisation concerned, the importance of the infrastructure in question and current threats. Funding will be set not only to meet legislative requirements and industry standards, but also to respond to technological developments and the growing demands on the availability and security of digital government services.

In addition to the continuous increase in funding, the required level of cyber security will also be achieved by optimising the use of existing capabilities and sharing them effectively, including the use of secure centralised solutions in both services and security. Where legal regulations allow, processes for drawing public funds to ensure cyber security will be simplified. Where appropriate, the public administration's needs in this area will also be met through public-private partnerships (PPP projects) or through funding from EU funds or other international sources.

Unifying Public IT Architecture and Strengthening Data Governance with an Emphasis on Security

IT architecture will be unified and systematic data management in the public sector will be strengthened to improve data security. Duplicate security and other solutions that generate unnecessary costs and provide no specific benefit will be reduced, and the interoperability of individual government systems will be deepened through the BIVOJ Project and similar solutions. Public institutions will have at their disposal the basic tools for secure and efficient processing of information in electronic form, in the form of comprehensive applications that can be used in various agendas with minimal additional configuration, and they will be motivated to use them.

Uniform rules will be introduced for the management, protection and use of data by the public administration to strengthen the transparency of public data, the protection of sensitive information and the coordination of data sharing among public authorities. Responsibility for the management, quality and security of data in public systems and areas will be established. The analytical usability of data will be enhanced for the effective performance of public administration, for working with open data, and for ensuring public oversight of public administration.

Promoting Secure and Resilient Supplies Beyond Strategic Infrastructure

Czechia will, while maintaining an open market environment, reduce the dependence of its strategic infrastructure on risky technologies and will prefer security solutions of domestic origin or from reliable partner and allied countries. It will promote the provision of secure and resilient supplies, diversification, and thorough screening of suppliers to strategic infrastructure. In order to enhance the protection of its systems against cyber threats, the state will, in selected areas, create new or integrate existing secure technology alternatives to solutions over which it does not have full control, including the implementation of open software and hardware solutions.

In view of the emerging trend of standardisation in cyber security, Czechia will also build competences in this area and support the establishment of certification bodies and testing laboratories.


Innovation
Competences
Education
Alternatives
Cooperation
Sustainability
Whole-of-Society
Preparedness
and Development

Strategic Area: Whole-of-Society Preparedness and Development

A high standard of knowledge, skills and cyber literacy throughout society is essential for ensuring the security of cyberspace and the prevention of human rights violations, especially among vulnerable populations. In accordance with the National Cyber Security Education Plan, Czechia will strive for the effective use of digital technologies by citizens and the continuous improvement of individuals' abilities to protect themselves and their environment from cyber threats through widely accessible education. Society-wide cyber resilience will also be built through a large, highly skilled expert base and effective cooperation across the public and private sectors, non-profit organisations and academia, as well as through civilian-military cooperation. Czechia will strengthen the role of research and development in cyber security with a focus on knowledge transfer to practice and the development of secure technological alternatives.

Strengthening Numbers and Motivation of Experts for the Long-term Sustainability of Czechia's High Level of Cyber Security

Specialised, high-quality cyber security training programmes and courses will increase the number of qualified graduates and experts. These programmes and courses will be inclusive and offer opportunities for different social groups to increase their professional representation in cyber security. Linking initial and further education will also ensure greater flexibility of the system in response to the labour market's real needs in this area.

Increasing the quality of working conditions – with a focus on financial and other motivation in expert positions where there is a shortage of personnel – will increase the attractiveness of work in cyber security for the government and strengthen the professionalism and stability of human resources in the public sector. Combined with the opportunity for career growth, the working conditions of experts in the public sector will move towards achieving competitiveness on the national labour market. Attention will also be paid to the equality of employment opportunities and conditions for women, experts without a university degree and graduates of non-technical disciplines in cyber security positions.

Public sector cyber security staff capacity will be managed economically, efficiently, and flexibly. By deploying emerging technologies and automating simple and routine activities, efforts will be made to increase added value and labour productivity, allowing the savings to be redirected to salaries within an organisation.

Development of Whole-of-Society Digital Competences and Cyber Security Culture

Enhancing education, prevention and awareness-raising in society will increase public knowledge of the safe and healthy use of digital technologies and their potential risks, including various forms of cybercrime, cyberbullying and online violence. It will strengthen the ability of public institutions, organisations and individuals to protect themselves in cyberspace, to critically analyse and evaluate information, and to make responsible decisions. Incorporating cyber security into education across all generations will foster the culture of cyber security in both work and private life.

Enhanced Cooperation to Coordinate and Overcome Differences Across Sectors

Information exchange and communication on cyber security between the public, private, non-profit, academic and civil society sectors will be strengthened. Through formalised platforms for cooperation and the active involvement of all relevant actors, cyber risks to the government and individuals will be reduced. This will make it easier to prevent cyber threats and deal with crises that have a society-wide impact in cyberspace. Building community and mutual trust, joint exercises, information sharing and coordinated response will enhance comprehensive cyberspace protection and increase mutual understanding of and alignment with the state's security needs. Civilian-military cooperation will also be enhanced to increase the state's situational awareness and improve efficiency and coordination among key actors, including mutual exchange of experience and sharing of good practices.

Developing the Knowledge and Skills of Cyber Security Experts

Conditions will be created for developing the competences of cyber security experts through formal and informal education, with an emphasis on the practical application of the knowledge acquired.

The education system and the range of further education courses will be developed and modernised to prepare both the general public and professionals for the challenges of navigating the digital world safely. Emphasis will be placed on updating teaching methods and ensuring the availability of materials and courses to respond to technological progress and emerging threats. Specialised, high-quality and attractive training programmes and courses will produce more cyber security experts and better security awareness in other specialties. The public, private, academic and non-profit sectors will actively participate in the development of this education.

Supporting Research and Innovation in Cyber Security

Czechia will support research, development and innovation in areas where it has a strategic interest or competitive advantage. Emphasis will be placed on the long-term sustainability and security of research results, as well as their applicability and transfer to practice. Acting in part through NÚKIB's role as the operator of the National Coordination Centre, the government will support activities linking academia, innovators and the public sector, in order to strengthen Czechia's position in the European research ecosystem. This will be achieved by ensuring appropriate cooperation between public authorities, the use of expertise, and adequate funding.

Cyber security will be one of the priority areas for dedicated support for research, development and innovation. In this context, NÚKIB will establish a professional structure for providers of state aid for research and development whose programmes focus on cyber security.

Promoting the Emergence of Secure Technological Alternatives

Czechia will support the development of new secure technological alternatives to strengthen both its own and the EU's resilience to supply chain cyber threats. This effort will support government, academic and non-profit entities, as well as relevant domestic industries and their competitiveness in national and foreign markets. To minimise dependence on suppliers of risky technologies, Czechia will, in addition to developing its own alternatives, actively seek joint solutions within the EU and NATO, and with other international partners, in order to share knowledge and resources needed to implement the principle of open strategic autonomy.


Partnership
Assertiveness
Transparency
Diversification
Sharing
Priorities
International Cooperation and Pursuit of Interests

Strategic Area: International Cooperation and Pursuit of Interests

Czechia's security is closely linked to international stability and to its membership of NATO and the EU, which remains the cornerstone of our security and defence, even in cyberspace. Responsible contributions to NATO capabilities and capacities, together with an active foreign policy, are and will remain key to advancing national interests and cyberspace security at both the national and global levels. Czechia will continue to promote adherence with public international law, with an emphasis on universal values and respect for human rights in relation to cyberspace. Czechia will continue to actively take action against cyber threats originating abroad and will not hesitate to respond accordingly.

Establishing New and Strengthening Existing Strategically Important Partnerships

Czechia will strengthen and develop cooperation with selected international cyber security partners, while maintaining NATO and EU cooperation as a priority. In NATO, Czechia will maintain its proactive approach, support the organisation's effectiveness and cohesion, and contribute to its activities.

When establishing, deepening or, on the conversely, loosening cooperation, Czechia will consider current and long-term international trends, its own national interests as well as those of its partners, including the promotion of shared democratic values. It will deepen cooperation, in particular, with the EU, across the Atlantic, in the Indo-Pacific region – with a focus on the IP4 countries, in the Middle East, including its multi-layered relationship with Israel, and with other like-minded partners. Czechia will continue its intensive diplomatic engagement through its cyber attachés and representatives in international organisations and EU institutions and will seek to expand their number and geographical presence.

As part of the development of international relations, and in response to trends in the international security environment, Czechia will continue to build new ties in abovementioned and other strategic regions.

Active Promotion of Czechia's Interests, Objectives and Priorities in Shaping International Rules and the EU Law

Czechia will contribute to the international development of secure cyberspace. Emphasis will be placed on the promotion of national interests and active participation in the development of international legal norms and standards. At the same time, Czechia will uphold those by all legal and diplomatic means and will not hesitate to speak out assertively against their violation.

Czechia will continue to play an active role in shaping EU and international regulations, conventions, treaties and standards in the field of cyber security. Through its active participation, it will help to ensure that international standards are set in a clear, appropriate and comprehensible manner and that they reflect Czechia's security and other interests and needs. Czechia will promote these principles both at the EU level, within other international organisations and groups, as well as in the national implementation of EU and international law. It will also actively promote the direct applicability of public international law in cyberspace in accordance with its 2024 national position on the interpretation and application of international law in cyberspace, which will be evaluated and updated as appropriate.

Czechia will actively advocate the protection and promotion of democracy and human rights in cyberspace and will actively and decisively speak out against threats to democratic principles in this area. It will continue to insist that states adhere to the norms of responsible state behaviour in cyberspace agreed by the international community within the UN, as well as to the common understanding of application of international law to cyberspace, as declared by the EU. These activities will include not only preventive measures, but also appropriate responses to harmful activities and human rights violations in cyberspace carried out by state and non-state actors.

Assertive Actions against Hostile Acts by Malicious Actors in Cyberspace, including Attribution of Attacks, Diplomatic Response and Imposing of Sanctions

Czechia will continue to use and strengthen its capabilities and capacities to attribute cyberattacks conducted by state or state-affiliated actors. In doing so, it will cooperate and coordinate its political-diplomatic steps and security measures with EU Member States and NATO Allies, and like-minded partners at the bilateral level. It will also make appropriate use of national and international sanctions mechanisms.

Through swift and assertive national and international responses to malicious activities in cyberspace, Czechia will seek to deter and punish malicious actors in order to indicate its ability and determination to act against those who seek to harm in and through cyberspace. By taking this approach, Czechia is demonstrating that it is not worthwhile for malicious cyber actors to target it, as the response by Czechia and its partners will outweigh any potential gains associated with hostile and malicious behaviour. Czechia will continue to strengthen its deterrence posture and will also actively promote this topic within NATO and the EU.

Promoting Open Strategic Autonomy

Czechia will actively develop its capacity to protect and promote its national interests in cyberspace, in line with the principles of open strategic autonomy, to better safeguard its digital infrastructure and data. This will include supporting the diversification of technologies, building expertise, and actively participating in shaping international policies on data protection, access to resources and technologies, and the protection of citizens' digital rights. Czechia will support these activities in international bilateral and multilateral relations, as well as within the EU and NATO.

Protecting a Global, Open, Secure and Free Cyberspace

Czechia will contribute to maintaining a global, open, secure and free Internet and cyberspace, based on the adherence to international law and built on the multi-stakeholder model. It will oppose efforts to control and fragment the Internet as well as it will actively advocate for its transparency and trustworthiness through cooperation among countries and with private and non-governmental organisations.

Strengthening International Information Sharing and Development Cooperation

Czechia will improve existing mechanisms for sharing know-how, information on cyber threats, vulnerabilities and incidents, as well as best practices among countries, organisations and other key actors at the international level. To this end, it will also make use of relevant NATO and EU mechanisms, including the NATO Integrated Cyber Defence Centre, responsible for raising situational awareness in NATO. This approach will, among other things, support the prevention of cyberattacks and enable a rapid and coordinated response, particularly within NATO and the EU.

In line with its own security interests, Czechia will give priority to developing strategic cooperation with the countries of the Western Balkans and the Eastern Partnership. It will also contribute as appropriate to building cyber security capacities in developing countries in other regions, such as sub-Saharan Africa, the Indo-Pacific, the Middle East and Latin America. This cooperation will include sharing know-how, training local experts and deploying our own experts to strengthen the stability, security and resilience of these regions in cyberspace. In its capacity building efforts, Czechia will leverage synergies and partnerships with other developed countries and funding from the EU, NATO and other external sources.

Support for Ukraine will remain an important priority of Czechia's international engagement in cyberspace, including assistance with the restoration of its digital infrastructure and the provision of technical assistance.

Implementation

The strategic objectives for the realisation of the NCSS' vision will be pursued through specific, measurable, achievable and time-bound tasks with designated persons responsible for their implementation. These tasks will be detailed in the NCSS Action Plan. The implementation of the NCSS Action Plan will be continuously monitored by NÚKIB, which will submit an annual evaluation to the Czech government.

The NCSS does not itself establish specific financial requirements for achieving its objectives. The implementation of the tasks in the NCSS Action Plan will be financed from the relevant chapters of the Czechia's state budget, EU funds and programmes, or through PPP projects.

While the implementation of the NCSS always depends on the current availability of resources in the state budget and other funding sources, investment in cyber security is an insurance policy that – compared to the costs of dealing with the consequences of attacks – will yield multiple returns for Czechia and will strengthen its competitiveness and economic growth.

Sources

1. Cybersecurity Ventures: The World's Third-Largest Economy Has Bad Intentions
   https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/

2. CBA: Czechs and Cyber Security 2024
   https://www.cbaonline.cz/clanky/cesi-a-kyberbezpecnost-2024

3. Check Point: Number of Cyber Attacks on Czech Companies Has Increased by 69 Percent
   https://cesky.radio.cz/pocet-kyberutoku-na-ceske-firmy-stoupl-o-69-procent-8834152

4. ENISA: Threat Landscape 2024
   https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

5. EU: Cyber Skills Academy
   https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

6. NÚKIB: Cyber Security Status Reports
   https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

National Cyber
and Information
Security Agency

NÚKIB