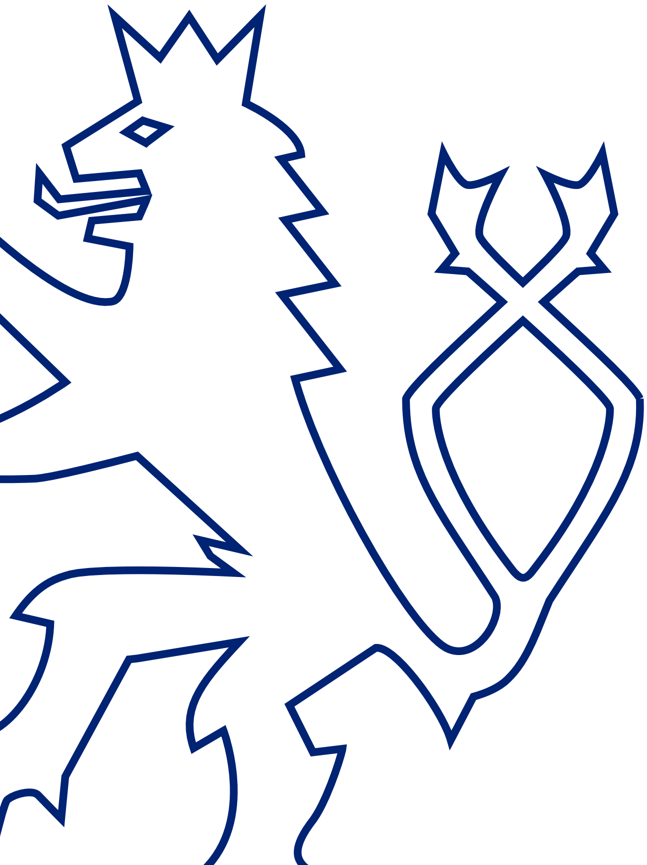
NATIONAL CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC



coordinated approach trust

attribution strong alliances

confident reactions

technological development threat detection

security strategic communication

CONTENTS

INTRODUCTION

Cyberspace and modern technologies have become inseparable parts of our lives. The gradual digitalization of Czech society is supporting our ability to compete, our economy, and our prosperity. On the other hand, it is also creating continually higher demands on cyber security, and today in 2020 the Czech Republic's interests are vitally dependent on cyberspace security. We live in an unpredictable security environment marked by turbulent social changes facilitated by technological developments. Lagging behind these developments would be dangerous and unacceptable, especially in terms of cyber security.

Since the beginning, the Czech Republic's approach to cyber security has been based on an effective model of cooperation between all relevant stakeholders at national and international levels, where each body has its own clearly set obligations and powers. This has made cyber security an important foreign policy subject in recent years. As a modern European country, the Czech Republic and our partners abroad will continue in these efforts and set trends in providing cyber security with the goal of finding a common path to maintaining a secure digital environment.

New threats demand innovative solutions. I therefore believe the Czech Republic will continue to successfully fulfil and implement the visions set out in the previous National Cyber Security Strategy. The country will strive to achieve the highest level of cyber security and ensure the conditions necessary for the smooth operation of an information society. Cyber defence will continue to be crucial – not just in terms of protecting critically important infrastructure elements, but also all other systems and networks. This will allow citizens to continue their activities and the state to pursue its economic and social interests. The most important aspect, however, remains enhancing the capabilities and capacities of all the state's security services, state institutions and organizations, associations, and individuals to face the growing threats in cyberspace. Resiliency is a fundamental pillar and basic prerequisite of an effective cyber security system for the Czech Republic.

The Strategy's main actors are the state's security services and other public administration bodies. However, the Strategy also supports and informs other parts of Czech society to enable them to better understand the state's actions when facing cyber threats and risks. It also serves as a source of information people can employ to use cyberspace and all modern technologies safely and reliably. I am convinced the new National Cyber Security Strategy will strengthen the Czech Republic's cyber security policy and create an excellent foundation on which to build.

Ing. Karel Řehka

NÚKIB Director

This Strategy fully respects the logical framework of the Methodology for Preparing Public Strategies and other recommendations. The Strategy is structured into three basic visions: (I) confidence in cyberspace; (II) strong and reliable alliances; and (III) Resilient Society 4.0 corresponding to the future strategic direction of the Czech Republic in coming years. These visions include definitions of fundamental principles that elaborate the idea behind the vision. Although it may appear that the Strategy is valid indefinitely, it will be updated in five years' time or in reaction to significant changes in the cyber security environment, and specific deadlines will be set for specific tasks laid out in the Czech Republic's Cyber Security Action Plan for 2021-2025 (hereinafter the "Action Plan").

SECURITY ENVIRONMENT: STRATEGIC CONTEXT

The Czech Republic finds itself in an increasingly complicated security environment that has been fundamentally transformed in recent years. A significant role is played by the critical dependence of the state and all of society on modern technologies and cyberspace.

Today, cyber threats have reached an unprecedented level, closely following the development of digital society. Some traditional security threats have migrated into the digital space, creating even more risks specific to this environment. Various threats have also been compounded, hybridizing the security environment as the dynamics and reach are expanded by cyberspace and modern technologies. All these threats have a common element: they are all so complex that they test the public's trust in the state and its institutions, and in extreme cases can upset the stability of societies and the democratic foundations of nation states. The chief prerequisite for introducing and implementing effective cyber security measures is the ability of the state and the security services to understand how threats dynamically develop.

Providing cyber security today goes well beyond mere technology, demanding a comprehensive approach. However, it is necessary to consider specific political, economic, social, cultural, and other aspects and interests when addressing cyber threats. Diplomatic, legal, educational, and other non-technical measures are necessary tools for fighting cyber threats and building a resilient information society.

The use of cyberspace to promote a country's foreign policy interests has intensified. The Czech Republic and its institutions have been cyber espionage targets for many years. Information acquired in such attacks can give the aggressor advantages in diplomacy, weaken the Czech Republic's negotiating position, and threaten its strategic interests. States do not just target public entities; there is growing interest in private entities such as small and medium-sized enterprises that have unique knowledge, as well as academia and research institutions. The increased risk of industrial espionage in business, academia, and research is tied to the development of Czech industry, and these impacts can significantly weaken our ability to compete.

Operational Domains

Cyberspace was recognized as an operational domain along with the ground, naval, and air domains at the 2016 NATO Summit in Warsaw. Space was acknowledged as another domain in London in 2019.

State and non-state (often supported or tolerated by the state) entities have undertaken malicious targeted offensive cyber operations. Cyberspace is a relatively new operational domain, and it is not surprising that military budgets for cyber activity are increasing across NATO member states and around the world. The growing importance of military operations in cyberspace has been objectively recognized, and an intensification of development in this area has been seen. As technology advances, non-state entities have increased their activities, while the commercialization of cyberspace means sophisticated cyber and kinetic operations do not only target the most advanced states. Less developed ones can participate and even dominate in this area. Automation, new computing models and concepts, and advanced machine learning with elements of artificial intelligence positively stimulate economies but also boost the effectiveness of asymmetric combat and enhance the offensive abilities of cyber security attackers as well as state and non-state entities.

The central challenge for the Czech Republic in this area is to concentrate not only on current cyber security threats, but also to acquire the ability to adapt to the new and constantly changing security environment. To achieve this, the Czech Republic must have the necessary capacities and constantly seek new ways to face current and future cyber threats.

THE CYBER SECURITY SYSTEM IN THE CZECH REPUBLIC

The structure of the cyber security system in the Czech Republic is complex. A significant number of bodies participate, each having its own role and contributing to cyber security in different ways depending on their powers and activities.

As the supreme embodiment of executive power, the government of the Czech Republic is responsible for ensuring national security and for the administration and operation of the entire Czech security system.

The National Cyber and Information Security Agency (hereinafter "NÚKIB") is the cyber security administrator and the central administrative body for cyber security, including the protection of classified information in information and communication systems as well as cryptographic protection. Its powers are determined by Act No 181/2014, on cyber security (hereinafter the "Cyber Security Act"), and legislation on the protection of classified information and security qualifications. It is also responsible for non-public services in relation to the Galileo satellite system. Of its broad range of activities, the central one is to ensure cyber security by protecting critical information infrastructure and other important communication systems and networks. The government CERT (hereinafter "GovCERT.CZ") was created to this end by the Czech government, while other NÚKIB parts provide mandated entities with various services. NÚKIB oversees international cyber security cooperation while also serving as the national contact point for coordinating research, while significantly contributing to cyber security education efforts.

Act No 181/2014, on cyber security and changes to related laws (the Cyber Security Act), as amended, is the first ever comprehensive Czech law covering cyber security. It primarily establishes obligations to ensure the security of cyber and informational infrastructure for selected public and private entities and individuals (mandated bodies and individuals). It also establishes NÚKIB's authority in coordinating and overseeing the provision of cyber security in the Czech Republic.

The national CERT works in close cooperation with GovCERT.CZ, and its powers are determined by the Cyber Security Act and a public contract signed with NÚKIB. The national CERT – under the name CSIRT.CZ – has been operated by the CZ.NIC association since 2011.

Foreign policy and relations between the Czech Republic and other states and international organizations are coordinated by the Ministry of Foreign Affairs of the Czech Republic (hereinafter the "Ministry of Foreign Affairs"), which cooperates with NÚKIB and other state bodies in cyber security.

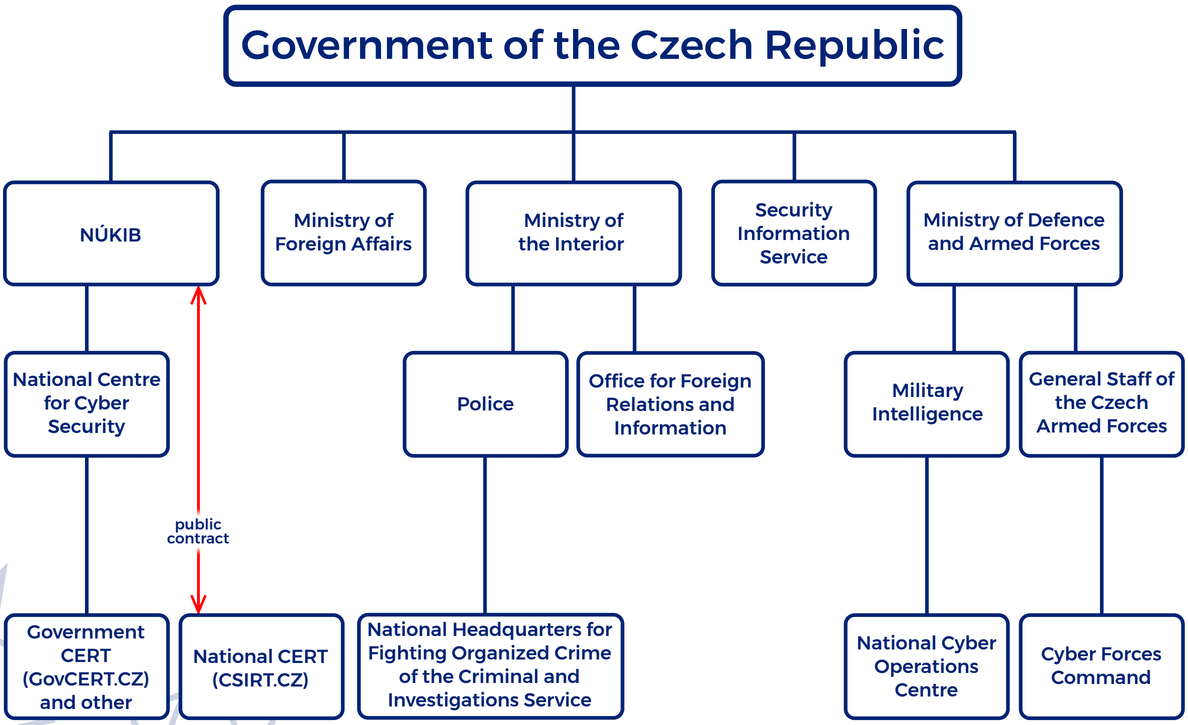
Intelligence services also contribute to the cyber security system. The Security Information Service is active in cyber security, as is Military Intelligence, and the Office for Foreign Relations and Information, which procure, process, and analyse information important for cyber security and hence national security in the Czech Republic.

The Czech Police, specifically the National Headquarters for Fighting Organized Crime of the Criminal and Investigations Service is the national contact point for cybercrime and for reporting malicious content on the Internet. The fight against and the prevention of cybercrime is primarily left to law enforcement bodies.

The ability to mount an effective cyber defence against the most serious threats is an area that is continuously growing in importance. Cyber defence is an autonomous and specific area of the wider cyber security concept in the Czech Republic, as well as part of the broader concept of ensuring the country's security. Compared to cyber security, cyber defence is chiefly characterised by the different nature of activities in cyberspace – and the different intensity of the attacks to which it reacts. Military Intelligence is responsible for building the cyber defence system in the Czech Republic.

The Czech Army, specifically Cyber Forces Command, participates in providing cyber security by acting independently and in coordination with ground, air, and special forces. The command and leadership of military cyber operations closely cooperates with Military Intelligence and their capabilities are mutually complementary.

Ensuring Cyber Security in the Czech Republic


Government of the Czech Republic
NÚKIB
Ministry of Foreign Affairs
Ministry of the Interior
Security Information Service
Ministry of Defence and Armed Forces
National Centre for Cyber Security
public contract
Police
Office for Foreign Relations and Information
Military Intelligence
General Staff of the Czech Armed Forces
Government CERT (GovCERT.CZ) and other
National CERT (CSIRT.CZ)
National Headquarters for Fighting Organized Crime of the Criminal and Investigations Service
National Cyber Operations Centre
Cyber Forces Command

The Czech Republic's cyber security system is not created purely through the above-listed institutions endowed with specific security mandates and agendas. The digital economy and the development of the telecommunications market are closely related to cyber security, meaning the roles of the Ministry of Industry and Trade and the Czech Telecommunications Office are also important. Other institutions also play vital roles, such as the Ministry of the Interior with its focus on building e-government services, and the Ministry of Education, Youth, and Sports and its influence on educating new generations of citizens, making it an intrinsic component for the successful functioning of the entire cyber security system. Other institutions of key importance in their particular fields are also incorporated into the system.

Representatives of bodies and individuals mandated under the Cyber Security Act play fundamental roles. These bodies have a significant influence on cyber security in the Czech Republic and the effectiveness of the overall system. They are responsible for their own security, which means fulfilling and upholding security principles and complying with relevant legislation. Similarly fundamental roles are played by bodies in the private sector, academic institutions, associations, groups, and CSIRT teams outside public administration that are not governed by the Cyber Security Act, even though their influence and seamless cooperation are key for the entire system.

1. CONFIDENCE IN CYBERSPACE

The Czech Republic has been a relatively safe and economically prosperous country for decades. It will be necessary to flexibly adapt to the newest threats for this to continue. Fundamental prerequisites of the Czech Republic's ability to defend itself in cyberspace are a comprehensive system to detect cyber threats using the abilities and capacities of the system's individual components; effective cooperation between national security and other bodies; and the coordinated, effective, and timely sharing of information. The risks of cyber threats to the state have grown in recent years, and so the Czech Republic must now react to a whole range of new technical, legal, and political challenges. The country will therefore act assertively and decisively in cyberspace at the government level. A confident, responsible approach to cyber security at the national level will promote the Czech Republic's prosperity and allow it to continue to act as a strong ally to its partners at the international level.

1.1 A Common Approach to Cyber Security

Ensuring cyber security involves coordination among many state and non-state bodies to enable the Czech Republic to effectively face even the most serious and complex challenges and threats. A common, integrated, and national approach to providing security in cyberspace and the fight against cyber threats is essential. The Czech Republic will therefore strive to improve the current model for identifying and detecting cyber threats, their subsequent analysis, and reaction to them. This will contribute towards effectively utilizing the capacities and capabilities of the relevant bodies, limit redundancies, and contribute towards the better use of human and financial cyber security resources.

The current complex security situation is increasing the demands placed on the foreign and security policies of states, including their ability to independently react to and resist cyberattacks. A united approach and understanding of cyber security and defence at all levels of political decision-making is thus vital for the effective management of crises and military situations in cyberspace, as well as for their prevention. Continuous efforts to improve cooperation and information sharing will contribute to finding consensus in the most important cyber security matters, both across individual state institutions and throughout the domestic political spectrum.

Civilian/military cooperation is also important for securing cyberspace. The national defence concept includes military support for civil society and civilian support for the armed forces. These efforts to create a fully functioning model for the country's cyber security need to continue. This model must be based on applicable legislation and procedural configuration to ensure individual bodies have clearly defined and mutually complementary powers. The mutual cooperation in setting functional processes between the civilian and military spheres must then be continually monitored through both everyday activities and specialized exercises and training.

Leaving cyber security solely to the Czech state is not enough, however. Every institution, private company, and individual has their role and can positively contribute to cyber security. The Czech Republic must therefore set up and support a cyber security policy that will consistently incorporate all of society into cyber security processes and thus increase its resilience to cyber threats.

Finally, the Czech Republic will continue to update its laws to create understandable, effective, and rational regulations concerning cyber security in order to be able to effectively react to current security situations, trends, and discoveries from the relevant technical and social sciences. This process will take place through the implementation of EU law into national legislation and the interpretation of binding international legal standards, to which the Czech Republic will continue to contribute.

1.2 Secure Infrastructure

The Czech Republic will continue to primarily focus on further increasing the resilience of its strategic information infrastructure. A culture of resilience will be created among all the bodies mandated through the Cyber Security Act on the basis of mutual trust and cooperation. They are the keystone of cyber and subsequently national security. Cyberattacks against the information and communication systems of these bodies and individuals could weaken and possibly have devastating results for the national economy, or limit the ability to provide for the population’s fundamental needs. The failure of one infrastructure component could lead to the failure of other parts, causing a domino effect. This is why their defence and security is of the highest priority for the country, and why it is necessary to continually increase infrastructure resiliency.

Due to the extensive automation and digitalization of industry, the cyber security of industrial management and SCADA systems has a specific position in the Czech Republic as the Internet of Things expands. These specific systems are often part of the state’s critical infrastructure. The Czech Republic thus aims to maintain their continual analysis and the monitoring of their security. In this respect, the country will continue to advocate the building of secure next-generation telecommunication networks, and thus continue the systematic and rigorous evaluation of the risks associated with creating and maintaining resilient infrastructure.

The Internet of Things

The name for a network of physical devices, such as cars, home appliances, etc., that are equipped with electronics, software, sensors, moving parts, and a network connection that allows them to connect to one another and exchange data.

Another trend that has taken root in the Czech Republic is the gradual shift towards cloud solutions in both the private and public sectors. This shift will also concern bodies mandated through the Cyber Security Act, and bring about not just new opportunities and expansion in functionality, but also increased demands on security. In this respect, the country must effectively react by establishing effective measures and overseeing their compliance.

Cyber security cannot be considered a purely technical matter. Reliable, secure, and resilient infrastructure demands a corresponding strategy, properly implemented policies and processes, a comprehensive legal framework, active cooperation, and adequate human resources – including knowledgeable and prepared management. A comprehensive view of cyber security is thus fundamental. Only when the Czech Republic evaluates cyber threats in a wider context can it effectively face them. A whole series of non-technical aspects therefore need to be taken into consideration when providing cyber security. Systematic and rigorous risk evaluation that includes both technical and non-technical aspects of cyber security is necessary to create and maintain resilient infrastructure. The basic question is supply chain security, meaning the need to determine whether external actors and individuals that influence the state's most important infrastructure are a risk to security.

The provision of high-level cyber security will entail corresponding costs that must be incurred not only to benefit national security, but also in association with requirements stemming from membership in international organizations. Sufficient financial resources are necessary to fight cyber security threats and secure infrastructure and technological development, and to offer prepared and trained experts adequate remuneration while providing for their ongoing training.

1.3 Effective Strategic Communication

The Czech Republic understands the importance of its strategic cyber security communication, which has significantly increased in recent years. The country's cyber security activities must be continually communicated with all national partners, including experts and the public. Intensive communication should be established, both domestically and internationally.

Strategic Communication

The state's strategic communication is synchronized activities, actions, and communication by individual state bodies to reach the target audience. It provides information coherently through unified messaging among all participating bodies over the long term. The goal is to prevent the abuse of an information vacuum for alternative interpretations.

In many cases, the goal of cyber attackers is not just an immediate negative impact on trust, integrity, or access to information and communication systems and devices. Attackers strive to achieve a psychological effect, and cyberattacks are used in various disinformation and influence operations. Their priority is to create uncertainty, fear, the feeling of a loss of safety in society, or to reduce civic morale and trust among citizens in public institutions and the overall democratic system.

The Czech Republic thus must understand the information environment that surrounds it and the dynamics and complexities of the cyber security threats it is facing. It can then establish a coherent dialogue and communication with the public. All acts by the state must be coordinated across all relevant state institutions to maintain citizens' trust in the state. Regularly communicating cyber security activities and the fulfilment of the Czech cyber security policy is important, as is preparation, agility, and the ability to react to a crisis.

Finally, the Czech Republic will reinforce digital hygiene principles, critical thinking, and media literacy in society. This will allow the country and its people to achieve higher resiliency to malicious manipulation inside and outside cyberspace.

1.4 Confident Reactions

The cyber security policy is an integrated part of the Czech Republic's overall security policy. The country will thus employ a proactive and decisive approach based on the timely detection of cyber threats, their expert analysis, and the immediate implementation of adequate countermeasures. The Czech approach to cyberspace primarily reflects a policy of actively preventing conflicts and the application of preventive diplomacy. In the event of a crisis or conflict stemming from aggressive or malicious cyberspace activities, the country is prepared to act immediately, forcefully, and to use all diplomatic, political, and – in extreme cases – military resources or sanctions against the aggressor.

One of the security pillars is NATO's principle of collective defence that counts on utilizing the national capacities and abilities of NATO partners, including in cyberspace. Membership in the EU and other international organizations, as well as bilateral cooperation, also contribute towards security. In light of the unique nature of the cyber threats to which the state has to immediately react, it is necessary to take responsibility for security and focus on the ability to independently and quickly respond. This will allow the Czech Republic to better defend itself from malicious aggressors and act as a more reliable partner in international relations.

Through its continual efforts to achieve the highest possible level of security, and its visible, confident reactions to cyberattacks, the Czech Republic will strengthen its overall resilience in cyberspace using the deterrence concept that is part of the current cyber security and defence system.

In this respect, attribution is a significant challenge. Determining the source and identity of an attacker is a basic prerequisite for any effective reaction. There are, however, a series of specific obstacles in cyberspace that make attribution difficult. The Czech Republic aims to minimize all the advantages cyberspace offers attackers. To this end, the country will focus on strengthening efforts and capacities in the national cooperation system, specifically in detection, timely reaction, and the establishment of a national attribution system for cyberattacks and other malicious activities in cyberspace. The majority of resources will therefore be invested in analysis and the coordination of results. This is the only way the Czech Republic can act confidently in cyberspace, and actively cooperate on attribution with its partners – both bilaterally and in international organizations.

Attribution

The process of ascribing, or attributing, a malicious cyber activity to a specific state or non-state actor. Attribution ideally takes into account technical, non-technical, and multi-source information. The information is then discussed and approved at the political level, which also decides on the action to be taken based on the attribution.

1.5 Future Challenges

In the 21st century, it is not enough to merely react to national security threats. The Czech Republic will take a proactive approach and strive to understand new threats as soon as possible, while creating resiliency and the capacities to fight against them. We are currently undergoing a fundamental transformation of the security space, intensified by the dynamic development of modern technologies. Artificial intelligence, quantum computing, and other modern concepts will lead to a paradigm shift in cyber security. It will also intensify the dependence of the state and society on modern technologies, while expanding attackers' options for malicious activity against the state, private entities, and individuals. A change in cybercrime capabilities and more sophisticated and technologically advanced methods of committing crimes, as well as an increase in the number of attacks can all be expected, as well as more ingenious cyberattacks by state and non-state entities. The coming years may bring an unprecedented transformation in the nature of conflicts, accelerated by the development of breakthrough technologies.

The Czech Republic must create the capacity to identify, analyse, and evaluate not just current, but also future cyber threats and risks that could endanger national security or social and economic prosperity. It is also necessary to begin differentiating the attributes of ordinary cybercrime and cyber espionage to optimize the conditions for law enforcement and intelligence services to fulfil their tasks.

The Czech Republic possesses excellent technical and technological cyber security knowledge. In order to be as resilient as possible to future attacks, the country must constantly monitor current affairs and remain active in research and innovation in new cyber security technologies, as should Czech industry. Cooperation with partners from the public, academic, and private sectors in research and development in technological and social science areas is thus fundamental. Research and development needs, problems, and priorities have to be clearly set with the goal of adequately reacting to the needs of society and users. The Czech Republic and its relevant state institutions must thus create a foundation for its partners that will strengthen knowledge-sharing and cooperation among individual entities.

2. STRONG AND RELIABLE ALLIANCES

A crucial vision for the Czech Republic as a modern European country is an active role in creating international dialogue, especially in the Euro-Atlantic space. The Czech Republic will base its approach on coherent national positions and clearly defined strategic interests. This foundation will be used to build strong alliances with partners in cyber security and defence.

2.1 Effective International Cooperation

Czech national security and prosperity is directly dependent on stable and secure access to cyberspace. Its specific open character allows modern threats and risks to easily cross national borders and act globally. International security is therefore one of the most important aspects of cyber security. Only active bilateral and international cooperation can meet the challenges of cyber security.

International cooperation in cyber security demands the incorporation of the national civil, military, public, private, and academic sectors. The basic prerequisite for the successful promotion of national interests and Czech security in the international environment is synergies in national positions. This unified approach will strengthen the country's active role in international organizations, forums, and conferences focused on advocating for Czech interests within the European Union, the North Atlantic Treaty Organization, the Organization for Security and Cooperation in Europe, the United Nations, and the Organization for Economic Cooperation and Development. Special emphasis will be placed on cross-border cooperation within the Central European region, where the Czech Republic will lead the dialogue.

Coordinated reactions and procedures to combat cyber threats with the goal of creating a resilient international reaction system are also important. The Czech Republic considers the ability to coordinate attribution and take effective measures based on common interpretations of international legal regulations as a major part of this system.

Support for an open, stable, and secure cyberspace will also be ensured through international efforts to create security evaluations of digital processes, products, and services that have become a regular part of society and carry a high security risk. The Czech Republic will support cooperation between governments across sectors and civil society while creating new cyber security standards. These will allow infrastructures and organizations to perfect their cyber defences and strengthen the security of digital processes, products, and services throughout their entire lifecycle and supply chain. Finally, the country will continue to actively participate in international discussions about Internet governance and international cyber security standards.

2.2 Deepening and Creating Active Partnerships

Bilateral partnerships form another fundamental component of international cooperation. The Czech Republic will continue to enhance its current partnerships in cyberspace and work towards more effective strategic partnerships.

These partnerships will be based on shared values, common interests, and unified positions to cyber threats. Bilateral cooperation will take place through various channels and will be strengthened by efforts to harmonize policies and approaches to cyber security within international organizations and platforms.

Detecting malicious activities performed by foreign powers with the goal of violating the sovereignty, territorial integrity, democratic principles, and laws of the Czech Republic and its partners is one of the challenges to strengthening the effectiveness of bilateral cooperation and incorporating unified approaches in practice.

The Czech Republic will continue to strengthen cooperation with selected allies through establishing and maintaining close cooperation with relevant foreign bodies and institutions, sharing strategic information, and active representation of the country in relevant international organizations and initiatives.

2.3 International Legal Framework

In accordance with its place in the Euro-Atlantic space, the Czech Republic remains resolved to protect the accessibility, openness, interoperability, reliability, and security of cyberspace.

As part of its interests and policies, the country will continue to actively contribute towards the creation of EU regulations, especially in light of the current challenges and needs resulting from the activities of state and non-state actors in cyberspace. It is thus primarily necessary to interpret new challenges and legal problems generated by technological development using the long-respected resources of national, international, and EU law, and to adapt state institutions' procedures to them.

A fundamental challenge for the Czech Republic and Euro-Atlantic states will be the creation of a unified approach to interpreting and applying public international law in cyberspace. The Czech Republic will continue to actively participate in this process, as it will in international discussions about non-binding norms of responsible state behaviour with the goal of actively contributing towards stable and responsible behaviour of states in cyberspace. The Czech Republic will emphasise the use of international law to protect human rights in cyberspace.

The Czech Republic will responsibly support and assist – in cooperation with partner states – in strengthening cooperation between law enforcement and other bodies providing supranational cooperation in the fight against cybercrime and enabling law enforcement.

2.4 Capabilities and Expertise

The Czech Republic confirms its willingness and responsibility to cooperate and actively aid international partners in strengthening security and defence. This will lead to the implementation of specific preventive measures to prevent malicious cyber activities by state and non-state actors.

The country will continue to share the knowledge and expertise it acquires through cyber security exercises, training, and other activities, while using appropriate tools to increase cyber security, and to establish and strengthen partner relationships. Besides exercises, the country will also focus on sharing legislative and strategic cyber security frameworks, especially with states that are only now establishing their own national cyber security structures.

The Czech Republic will continue to emphasize support for strengthening cyber security capacities to fight cyber threats in partner states. In the borderless territory of cyberspace, it is necessary to view threats as a global problem, where a threat in a foreign country could eventually affect the Czech Republic. It will also contribute expertise in this area to help developing states increase their resiliency.

The country is prepared to share its capabilities and expertise with partners, especially with less developed states that are still building their cyber security capacities. Strengthening the cyber security abilities of individual states at the national level will increase their resiliency and prevent the possible abuse of their infrastructure by attackers to commit malicious acts in cyberspace.

3. RESILIENT SOCIETY 4.0

The Czech Republic is a European leader in the dissemination and use of modern technologies. As a result, Czech society is successfully transforming into an information society. This established trend has also brought about both an increase in the number of end users in Czech society and the risks to which those users are exposed. Insufficient digital hygiene, media literacy, and critical thinking are problems across society associated with this growth. The country must thus focus on the successful transformation of Czech society into Society 4.0: a state where cyber threats are minimized and all of society can leverage the benefits of modern technologies and integrate them into their everyday lives. Cyber security must thus remain an intrinsic part of people's everyday lives.

Digital Hygiene

A set of principles, procedures, and habits that allows users to securely move around cyberspace. This is a proactive approach by users to their digital footprint, security, etc.

3.1 Securing Digital Society and Public Administration

The Czech Republic has been striving to digitalize its public administration for several years. Building a digital infrastructure for public administration must take place with extreme emphasis on cyber security from the very beginning. The operation and administration of this infrastructure must also be accompanied by a high level of security. It is therefore necessary to reflect the current security situation, regularly perform coordinated and continual risk analyses, and use the results to apply the necessary measures.

The digital infrastructure will be built with the goal of assuring the mutual compatibility of the technologies used in the individual public administration areas. Here, the country will continue to support the use of unified information channels that allow for secure data exchange.

Another key characteristic of digital infrastructure is resilience. The state must guarantee the smooth operation of infrastructure under all conditions. Despite this resiliency, it is necessary to create alternative methods of providing services in cases where the state administration is not able to do so electronically.

3.2 Education and Awareness

Cyber threats, the spread of modern technologies, and their incorporation into society have become intrinsic parts of every citizen's life. The Czech Republic must thus reflect this situation and include cyber security at all levels of the education system and across all fields. It is necessary to emphasise security as a priority when using any electronic device.

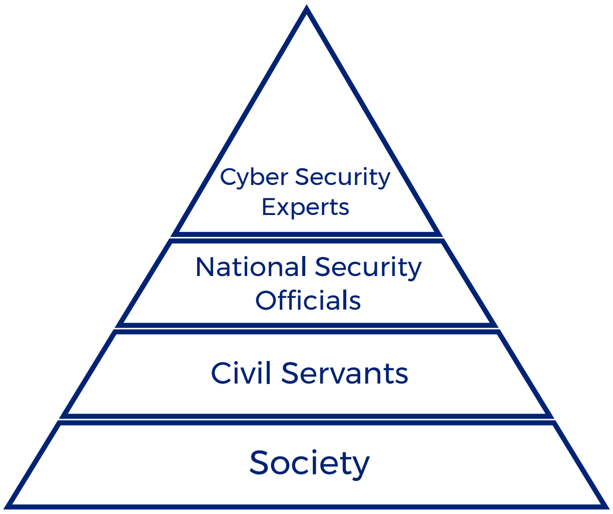
Implementing a high-quality and modern education system is necessary to strengthen the country's overall cyber security. Starting at the pre-school level, education projects that aim to teach safe Internet habits and the use of digital technologies will be promoted.

Besides children and students, the state will also focus on educating other selected target groups, specifically educators and civil servants. Educators are a key building block of the education system, and providing them with knowledge about cyber security is necessary to develop information literacy among children and students, as well as the teachers themselves as citizens. This will significantly help the education system adapt to this topic. Educating civil servants will contribute towards greater resiliency to cyber threats among public administration bodies. End users are a popular target for cyberattacks. In this respect, the Czech Republic must be able to provide the appropriate support for specially educated experts to contribute towards improving national cyber security as well as to educate and raise awareness in other relevant groups.

Elderly people are another important population segment exposed to the negative impacts of modern technologies. They need to be educated, especially in the safe use of digital technologies and in recognizing disinformation. Besides the elderly, other high-risk groups across generations also need to be educated, which will require specific targeting.

Other educational activities will continue to include either broadly or narrowly targeted awareness campaigns. The responsible state bodies, with contributions from the private, academic, and non-profit sectors, will significantly help spread cyber security awareness. These campaigns will not just increase awareness about cyber security, but will also build trust through their open nature familiarizing and describing the activities of state bodies as well as those in the private and academic sectors.

A Resilient Cyber Security System



3.3 Expanding the Qualified Base

The Czech Republic will actively create and maintain a qualified cyber security workforce and thus develop its foundation of educated and motivated people as one of the state's most valuable resources. This means the country must act on two basic levels.

The first level is the identification of talented people and motivating them to study and work in cyber security. It is therefore necessary to systematically invest in modern education and awareness programs and to coordinate those efforts with the academic sector. At the same time, state bodies must invest in creating the appropriate working conditions. The state administration must be able to compete on the highly competitive cyber security labour market. It has to create working conditions that motivate emerging talented people to work for state organizations and the state security services.

The second level is a proactive approach towards selected individuals. In this area, state bodies must work to retain their cyber security staff. To achieve this, the appropriate working conditions need to be created. This is not simply about remuneration, but also about creating an effective motivation system with internal education, a career path, and the appropriate conditions to compete.

Besides these two basic levels, all other recognized experts who work outside state administration should be allowed to participate in ensuring cyber security in the Czech Republic. Leveraging their capabilities will be institutionalized in an appropriate way, primarily in case of a serious threat to the Czech Republic that requires more human resources than the state usually has available. This system of incorporating cyber security experts from outside state administration will help create an accessible and qualified group of volunteers. In this way, the Czech Republic will offer work to experts from the private, non-profit, and academic sectors.

STRATEGIC GOALS

Vision		
The Czech Republic will have a resilient society and infrastructure, will act confidently in cyberspace, and will actively confront the entire spectrum of cyber threats while strengthening reliable alliances.		
Confidence in Cyberspace	Strong and Reliable Alliances	Resilient Society 4.0
Strategic Goals		
• A national approach emphasizing information sharing, coordination, and cooperation • Developing state cyber security capabilities and capacities • Strengthening the security and resiliency of infrastructure • Developing prediction, detection, and agile reactions to cyberattacks • An effective communication strategy • Preventing and fighting cybercrime	• Effective international cooperation • Creating alliances • Promoting Czech interests abroad • Creating dialogues in the international environment • Supporting open and safe behaviour in cyberspace • Exporting knowledge	• Ensuring the security of state administration / eGovernment digitalization • A high-quality education system • Raising awareness • Cooperation between the state, the private sector, and citizens • Creating a broad base of experts

IMPLEMENTATION

The National Cyber Security Strategy of the Czech Republic is, in a more detailed form, translated into specific tasks in the Action Plan. Both documents have been created in coordination with the relevant bodies responsible for the fulfilment of individual goals in the major cyber security areas. The National Cyber and Information Security Agency (NÚKIB), as the administrator of cyber security in the Czech Republic, will continually monitor, discuss, evaluate, and coordinate the fulfilment of these individual goals. This evaluation of cyber security by NÚKIB will be presented through the Report on the State of Cyber Security in the Czech Republic for the relevant years, an appendix of which will include a report about the fulfilment of the Action Plan.

LIST OF ABBREVIATIONS USED

CERT – Cyber Emergency Response Team

EU – European Union

GovCERT.CZ – Government CERT

NATO – North Atlantic Treaty Organization

NÚKIB – National Cyber and Information Security Agency

OSCE – Organization for Security and Cooperation in Europe

OECD – Organization for Economic Cooperation and Development

UN – United Nations