NATIONAL SECURITY AUTHORITY

The National Cybersecurity Strategy 2026 - 2030

FOREWORD

Roman Konečný

director
National Security
Authority

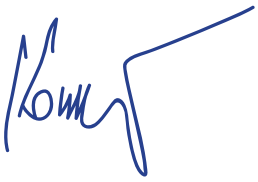
In recent years, cyberspace has established itself as a strategic environment in which significant security, economic and societal interests of the Slovak Republic are concentrated. The dynamics of cyber threats, their increasing sophistication, and their interconnectedness with other forms of hybrid influence place high demands on the ability of the state, public institutions, the private sector, and individuals to effectively prevent incidents and manage their consequences.

The National Cybersecurity Strategy of the Slovak Republic for 2026-2030 provides a framework through which the Slovak Republic systematically strengthens its resilience against cyber threats. It builds on the experience of the previous period, reflects changes in the security environment, and takes into account obligations arising from the Slovak Republic's membership in the European Union and the North Atlantic Alliance.

The aim of the strategy is to create the conditions for the coordinated and sustainable development of cybersecurity, based on clearly defined competencies, responsibilities, and cooperation mechanisms. It places particular emphasis on prevention, early detection of threats, effective incident management, and the systematic enhancement of the level of preparedness of all relevant stakeholders.

Cybersecurity is not merely a technical issue, but a long-term process that requires strategic planning, investment in professional capacities, and continuous risk assessment. The successful implementation of this strategy requires active cooperation across ministries, local and regional authorities, academia, and the private sector, as well as open dialogue with international partners.

I believe that this strategy will contribute to strengthening the security of Slovak cyberspace and will create a solid foundation for a responsible and coordinated approach to addressing the challenges that this environment will bring in the coming years.



CONTENTS

I. INTRODUCTION

The functioning of a modern digital society requires trust in technology and its security, in which the state plays a key role. A particularly significant development is the rapid advancement and deployment of artificial intelligence. Introducing these elements into the digital environment can increase the effectiveness of public policies, improve the quality of services, accelerate development and research, streamline industry and improve the everyday lives of citizens. In this area as well, cybersecurity is a fundamental factor in achieving a high level of quality in state governance, maintaining the constitutional and legal order of the state, democratic society and economic growth. **The National Cybersecurity Strategy of the Slovak Republic for 2026-2030** (hereinafter referred to as the "National Strategy") **is a fundamental document that defines priorities and objectives** so that an appropriate level of cybersecurity can be achieved in the coming period, taking into account the development of new technologies and threats that come with them.

The National Strategy sets out strategic objectives **in five priority areas:**

1. **Protection of national cyberspace**
2. **Building national capacities**
3. **Secure and innovative digital products and services**
4. **Education, skills and awareness**
5. **Strategic partnerships and international cooperation**

The proposed strategic objectives respond to internal and external factors that currently affect cybersecurity in Slovakia. They take into account the results achieved in the previous period and the current state of cybersecurity, as well as the dynamics of future developments, whether in terms of security threats or technologies.

II. External factors affecting cybersecurity

Geopolitics and International Relations

Cyberspace is a domain of global politics and the overall security environment. The digitalisation of states, including their economies and public services, means that the stability and resilience of cyberspace as such directly affects national and international security. This trend will not slow down in the coming years, and its pace will be determined mainly by the growing polarisation of ideological groups, technological rivalry between superpowers, and intense competition for control over data and information flows.

From the perspective of the strongest external factors, **the current security situation** in Europe is fundamentally influenced by the **ongoing armed conflict between the Russian Federation and Ukraine**, which also shows that cyber operations are an integral part of modern military and political action. During the conflict, there have been widespread cyber attacks on energy networks, media and state institutions in the European Union (hereinafter referred to as the „EU"), as well as targeted campaigns aimed at manipulating public opinion. Such developments are therefore contributing to changes in security doctrines in Europe and reinforcing the need for a comprehensive approach to cyber defence and security.

The ongoing tensions in the Middle East, in particular the continuing regional conflicts between Israel and Iran and militant Muslim groups, have, among other things, had a direct impact on the internal security of the EU and contribute to increased activity by terrorist and hacktivist groups in the broader context of hybrid threats.

Alongside these conflicts, **the influence of the People's Republic of China**, which has enormous human, economic and technological potential, is growing. China, which is undoubtedly a dominant power in Asia, is gradually becoming a global power, and its centrally controlled policy also influences other parts of the world, including Europe. China is not only an important trading partner for Europe, but also a technological rival. Its rapid development in the field of emerging and breakthrough technologies, given the political system in which they are applied, poses numerous challenges for democratic states, not only in terms of technological autonomy and credibility, but especially from a security perspective. China is also gaining more influence than in the past i**n international organisations**, including those focused on technology (such as the International Telecommunication Union (ITU) and other standardisation bodies).

At the same time, **the United States is re-evaluating its relationships** with global partners. This effort to optimise its own influence reduces the predictability of its foreign policy and leads to the conclusion that, in some cases, American leadership cannot be unconditionally relied upon on the international stage. The changes are also evident in the functioning of international organisations such as the United Nations (hereinafter referred to as the "UN"), the United Nations Educational, Scientific and Cultural Organisation, the Council of Europe, the Organisation for Security and Co-operation in Europe (hereinafter referred to as the OSCE), which is putting pressure on the EU to strengthen its strategic autonomy and increase investment in its defence and cybersecurity.

As a result, the EU feels more threatened today than ever before. The security environment is disrupted by hybrid operations, including foreign manipulation and interference in the information space, cyber attacks on its critical infrastructure and democratic institutions. Additionally, new risks are arising from climate change, environmental degradation and potential pandemics, which may have a secondary impact on digital and critical infrastructure.

The position of the Slovak Republic in the geopolitical arena

The Slovak Republic is an integral part of Western civilisation, based on the principles of democracy, the rule of law, fundamental human rights and freedoms. **Cooperation** with key partners **at European, transatlantic and global level**, as well as consistent respect for the international order and its norms, strengthens its contribution to collective resilience and contributes to promoting the EU's common narrative, of which cybersecurity is an integral part.

Security guarantees for the Slovak Republic are primarily provided by the North Atlantic Treaty Organisation (hereinafter referred to as „NATO") and the EU, which provide strategic, technological and security support for, among other things, joint projects, information exchange and coordination of responses to cybersecurity incidents. The Slovak Republic is also strengthening its ties and actively contributing to the activities of **the OSCE, the Organisation for Economic Co-operation and Development** (OECD), **the ITU, the Council of Europe** and **the UN**, which play an important role in shaping international standards and policies in the field of cybersecurity.

Cyber threats and trends in their development

The Russian Federation, the People's Republic of China, the Democratic People's Republic of Korea and **Iran** remain the dominant state actors posing threats in cyberspace. These countries have long used cyber operations as a tool for political, intelligence, military and economic action. Their activities are supported by the state and often carried out by groups that focus on advanced persistent threats (so-called APT groups), i.e. highly organised units that target the networks of public institutions, strategic companies and critical infrastructure. The aim of their activities is to gain access to sensitive information, gain political influence, undermine confidence in democratic institutions, destabilise society or cause economic damage to competitors.

However, there are certain differences between the various entities. **Russian groups** focus mainly on hybrid operations, combining **disinformation campaigns, cyber attacks** and **psychological operations** with the aim of weakening the unity of the EU and NATO. **Chinese activities** are mainly **intelligence-economic in nature**, focused on acquiring intellectual property, technological know-how and eroding supply chains. **The Democratic People's Republic of Korea** uses cyber attacks as a tool **to secure the regime's finances**, typically through cryptocurrency theft and ransomware attacks. **Iranian activities** often have a **regional and ideological** dimension, with targets mainly in the energy and public administration sectors.

According to the **ENISA Threat Landscape 2025** report, which analysed more than 4,800 incidents between July 2024 and June 2025, **state-sponsored groups and cybercriminal networks** remain the main perpetrators of attacks against EU Member States. **The most frequent targets** are **public institutions** (more than 1/3 of incidents), followed by the **energy, transport, healthcare and financial services** sectors. There is also growing c**onvergence in the tactics and tools** used by state, criminal and activist groups, including overlapping motivations, sharing of tools and outsourcing of attack capabilities between different types of actors.

Another significant trend is the increase **in attacks carried out by hacktivists** (mostly **DDoS** – distributed denial-of-service attacks), which have an ideological or political background and are increasingly overlapping with the agenda of states or allied entities. This phenomenon confirms the transition from isolated cyber attacks to **coordinated hybrid operations** that combine digital and information activities.

In addition to state actors, non-state actors also play a significant role – **hacktivists, organised cybercrime and private entities** whose motivations range from ideological to financial. The rapid growth of the cybercriminal ecosystem has led to the emergence of the „cybercrime-as-a-service" model, in which attack tools or access data are offered for sale or rent. This model significantly lowers the technological barrier for new perpetrators and increases the overall volume of cyber attacks.

These threats pose **a complex challenge** for **the Slovak Republic**. Attacks on public institutions, local governments, universities, energy and financial companies confirm that the state and the private sector are exposed to the same types of risks as larger European countries. Protection against these risks requires **strengthening intelligence and operational cooperation, coordinated threat monitoring**, systematic **risk assessment** and rapid **exchange of information on cybersecurity incidents** between national and European authorities.

Technological trends and globalisation of supply chains

QUANTUM TECHNOLOGIES

The European Commission has issued **a Recommendation on a Coordinated Implementation Plan for the Transition to Post-Quantum Cryptography**, which aims to ensure a uniform and gradual transition by Member States to quantum-resistant cryptographic solutions. Based on this recommendation, a **Coordinated Implementation Plan for the Transition to Post-Quantum Cryptography** was subsequently developed, which serves as a framework for a coordinated transition to quantum-resistant encryption. This roadmap sets out the basic principles, stages and responsibilities of Member States in **adapting to post-quantum cryptography** (hereinafter referred to as "PQC") according to the level of criticality of the sectors and systems. Building on this initiative, the Slovak Republic's strategic objective is to prepare and implement measures for the transition to PQC. Relevant actors across the public administration, private sector and academia should be involved in this transition. The National Security Authority will provide methodological assistance in the transition to PQC algorithms and will also issue a specific strategy for cryptographic protection and transition to PQC, which will include specific objectives and tasks in this area. As part of these measures, the National Security Authority has already issued **Recommendations for Cryptographic Algorithms**, which aim to raise awareness and increase the use of modern and proven cryptographic algorithms with an emphasis on high security and resistance to quantum threats.

The development of quantum technologies is fundamentally changing the cybersecurity environment. With their computing power, quantum computers could theoretically break the most widely used asymmetric cryptographic algorithms, including those based on the discrete logarithm problem and elliptic-curve cryptography, which form the basis of trust and security in digital communications, electronic services and data protection. This shift creates **a need for a timely transition to new PQC mechanisms** that will remain secure even in the era of quantum computers.

Attacks of the "steal now, decrypt later" type pose a serious threat, as currently sufficiently encrypted data may be decrypted in the future using quantum computers. For this reason, **it is essential** to prepare in advance for potential threats arising from the development of quantum computers and **to apply existing PQC algorithms**, especially in critical systems, and to invest in the transition to secure and resilient cryptography.

The transition to PQC will take place gradually, based on applicable legislation and in accordance with standards. Cryptography is not based solely on standards, technical solutions and their correct implementation. If the area of cryptographic information protection is not sufficiently covered by legislation, this may lead to the incorrect or non-implementation of appropriate measures by system and service operators, or to the incorrect interpretation of obligations arising from legal regulations. Therefore, proper legislative anchoring of this issue is essential for the correct implementation of technical security measures related to cryptography. For the private sector, the possible implementation of measures for the transition to PQC is of a recommendatory nature and, in order to prevent so-called gold-plating, their binding nature for the private sector will be subject to valid European legislation.

ARTIFICIAL INTELLIGENCE, PRODUCTS WITH DIGITAL FEATURES, AND CYBERSECURITY

Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules in the field of artificial intelligence (**Artificial Intelligence Act**) is considered to be the first comprehensive framework regulating the use of artificial intelligence and aims to become a globally recognised standard in the field of artificial intelligence regulation.

The Artificial Intelligence Act is closely linked with Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (**Cyber Resilience Act**). However, both regulations explicitly refer to each other, precisely for the purpose of ensuring the cybersecurity of high-risk artificial intelligence systems. Artificial intelligence systems are to be subject to a comprehensive and coherent cybersecurity regime. At the same time, this harmonisation must not lead to a reduction in the level of protection provided by the Cyber Resilience Act for important and critical products with digital elements. The aim is to reduce the regulatory burden while increasing legal certainty for manufacturers of high-risk artificial intelligence systems, particularly in complex cases where artificial intelligence and cybersecurity are blended together.

The Cyber Resilience Act is European legislation aimed at increasing the security level of all products containing digital elements, with the exception of products covered by other EU regulations (e.g. medical devices, cars, etc.). The practical implementation of the measures will lead to enhanced cybersecurity, as products with digital elements will only be allowed to be placed on the market after all known exploitable vulnerabilities have been removed. The manufacturer of these products is obliged to guarantee the same level of cyber resilience throughout the development and entire expected life cycle of the product.

Artificial intelligence is one of the most significant technological trends of our time, fundamentally changing the digital environment and the way society functions.

Artificial intelligence systems complement or replace traditional systems, opening up entirely **new uses, capabilities and services** that were not previously possible. In doing so, they are transforming entire industries. At the same time, however, understanding of the threats posed by artificial intelligence is still evolving, and research is constantly revealing new challenges, threats and vulnerabilities. This combination poses a significant risk to cybersecurity, especially if the introduction and use of artificial intelligence is uncontrolled and without awareness of responsibility and clearly defined rules.

The use of artificial intelligence also makes a significant contribution to strengthening the protection of the digital space. It enables faster and more accurate detection of cybersecurity incidents, more effective threat analysis, processing of large volumes of data and support for forensic analysis. Due to these capabilities, it increases the effectiveness of responses to cybersecurity incidents and contributes to the protection of individuals, organisations and critical infrastructure.

Artificial intelligence systems are changing the nature of attacks by contributing to **the automation of phishing, the generation of malicious code, the identification of system vulnerabilities, the circumvention of detection mechanisms**, and analysis of user behaviour in order **to tailor social engineering attacks** to their habits and behaviour. There are also forms of malware that use artificial intelligence mechanisms and dynamically change their behaviour depending on the defence mechanisms identified set up in systems or the behaviour of system administrators. These phenomena, also known as **"weaponisation of artificial intelligence", pose a major challenge to cybersecurity.**

Artificial intelligence already plays a significant role in **information operations**. Artificial intelligence systems are capable of automatically generating a large number of posts on social networks, often with the aim of influencing users or conducting information operations. The ability of artificial intelligence to create realistic **"deepfake"** videos, imitate voices or generate credible websites undermines trust in the public sphere and makes it difficult to distinguish reality from manipulation.

Another challenge is **the internal vulnerabilities of artificial intelligence systems themselves**. Manipulation of training data, such as input databases (data poisoning) and input modification, can lead to erroneous or deliberately misleading outputs. Unlike traditional software, where abuse is mainly possible after the system has been deployed, with artificial intelligence, the risk can arise during the learning phase, which significantly complicates the detection and mitigation of such vulnerabilities.

Last but not least, **it is important to address regulatory and ethical dilemmas**, as the rapid development of **artificial intelligence requires robust frameworks for responsible use** (transparency, controllability and protection of human rights) in line with the European approach known as **"human-centred, trustworthy artificial intelligence"**.

5G/6G

The deployment of 5G/6G technologies is already significantly expanding, and will continue to expand, the possibilities for using digital connectivity across society and the economy. This modern infrastructure enables **the development of new products and services** that are transforming the functioning of healthcare, transport, energy, public administration and industry. It fundamentally expands **the connectivity** of the Internet of Things. In industrial use, it provides a key foundation for **the development of the Industry 4.0 concept**, based on the interconnection of smart devices, robotics, artificial intelligence and the Internet of Things, which enable the automation and optimisation of production processes.

However, such a connected environment also brings **new risks**. 5G networks carry vast amounts of sensitive data and form the basis of critical digital infrastructure, while their **less centralised architecture, greater dependence on software, network and application interfaces**, and the need for a larger number of devices create **new entry points for attackers**. Ensuring their security and resilience is therefore essential not only for the protection of users, but also for the stability of the economy and society.

The next generation, **6G networks**, will bring even **deeper integration of communications, sensor functions** and **connectivity with satellite infrastructure elements**. Wider use of very high frequencies and new architectures is expected, which will increase the demands on data protection, authentication and device reliability. **These networks will increasingly be managed by machine-learning algorithms**, which will need to be protected from manipulation and misuse. **Preparedness for quantum threats**, device and node security from the design stage onwards, and rigorous cryptographic key management will also be priorities. The deployment of 6G networks is expected to begin around 2030.

SUPPLY CHAIN SECURITY

Supply chains are now an integral part of digital infrastructure, ensuring the lifecycle of products and services, from development and production, through distribution and maintenance, to decommissioning. Their stability and resilience are essential for the smooth functioning of critical sectors such as energy, transport, healthcare, telecommunications, finance and public administration.

Currently, information and communication technology supply chains are **highly complex because of global commercial interdependence** and are subject to multiple legal systems. This interconnectedness creates dependencies on external partners, **increasing the risk of vulnerabilities being transmitted** across the entire system. Even a single broken link in the chain can have serious consequences. **A failure in a supplier's cybersecurity creates an attack vector** that can have negative impacts across the entire chain, from data leaks to the interruption of key services.

Any policy that does not promote supplier diversification, support the European technology base and technological sovereignty, or create mechanisms for rapid response in the event of vulnerabilities being identified will have a significant negative impact on the EU and the Slovak Republic.

Dependencies on high-risk suppliers should also be treated as a distinct category of risk. This also applies **to innovative technologies such as PQC and artificial intelligence**, which may **pose an unacceptable risk** to the security of the entire ecosystem.

The management of the information and communication technology supply chain must also include a coordinated risk assessment system and maximum transparency, in particular through product security certifications, auditability requirements and the sharing of information on the origin of components.

III. Internal factors affecting cybersecurity

The state of cybersecurity in the Slovak Republic

The present National Strategy is the third strategic document aimed at building and strengthening the cyber resilience of the Slovak Republic. Since the adoption of the first Cybersecurity Concept in 2015 and the National Cybersecurity Strategy for 2021-2025, the Slovak Republic has taken significant steps to improve its level of cybersecurity.

First and foremost, a **legal and institutional framework** for the management and regulation **of cybersecurity at the national level** has been established. A stable legal environment defines the division of competences and responsibilities.

The hierarchical structure of cybersecurity management is overseen by the National Security Authority as the independent central government body for cybersecurity. **The National Cyber Security Centre** (hereinafter referred to as „NCSC"), as part of the National Security Authority, is continuously **strengthening the capabilities of its national CSIRT (SK-CERT) unit** in the area of prevention and response to serious cyber incidents at national and international level.

From a cybersecurity regulation perspective, **public administration** represents a significant part of national cyberspace. This sector is regulated by the Ministry of the Interior of the Slovak Republic (public administration entities at the level of the central state administration and other state authorities with nationwide jurisdiction and public administration entities at the regional level, except for the area of financial administration), the Ministry of Finance of the Slovak Republic (public administration entities in the area of financial administration) and the Ministry of Investment, Regional Development and Informatisation of the Slovak Republic (administrators and operators of public administration information systems). The Ministry of Investment, Regional Development and Informatisation has established a government CSIRT unit (CSIRT.SK), which provides preventive measures for the public administration sector and responds to cybersecurity incidents in this sector.

The Cyber Defence Centre of the Slovak Republic, as a special organisational unit of Military Intelligence, which is part of the Ministry of Defence of the Slovak Republic, **performs tasks in the field of cyber defence**, but also acts as a sectoral CSIRT unit for organisations falling under the remit of the Ministry of Defence.

The **area of cyber diplomacy**, coordinated by the Ministry of Foreign and European Affairs of the Slovak Republic, is also important.

The effective functioning of this ecosystem is ensured by mutual cooperation between the individual components within the scope of their legally defined competences and tasks.

The National Cybersecurity Strategy for 2021-2025 defined the following strategic objectives

- a trustworthy state prepared for threats,
- effective detection and investigation of cybercrime,
- a resilient private sector,
- cybersecurity as a fundamental part of public administration,
- strong partnerships,
- educated experts and an educated public,
- development of research and innovation in cybersecurity.

An analysis of the fulfilment of these objectives shows **progress in many areas.** Improvements are particularly noticeable i**n the areas of legislation, coordination and community building across the public and private sectors, improving the response to cybersecurity incidents** and **increasing the cyber resilience of operators of essential services**.

However, significant differences in the level of security between sectors remain, with the main challenge being to ensure the required level of security in the public administration, healthcare and education sectors. In these sectors, insufficient financial coverage of cybersecurity costs is also a problem. The problem of a lack of available resources for investment is partially offset by EU grant programmes, which, however, can only be used for predefined purposes. Such funding does not appear to be systematic. At the same time, there is a persistent **problem with human resources**, particularly with the recruitment of cybersecurity specialists, who are not sufficiently remunerated (especially in the public administration sector).

Education, science and research system

The current education system in the field of cybersecurity can be considered inadequate. Therefore, systematic development from basic education to higher education is extremely desirable and necessary. **In the Slovak Republic, several institutions, mainly universities, are addressing the issue of cybersecurity**, but there is no unified and coordinated approach. Universities develop educational programmes and research activities in this area in various ways, but without a comprehensive link that would ensure long-term cooperation and synergy between the academic, public and private spheres. Basic awareness of cybersecurity must begin in primary school and be further developed in secondary education.

The education system currently takes limited account of the fact that cybersecurity is not exclusively a technical field. The cybersecurity sector also relies on experts from fields beyond IT, such as lawyers, project managers, process analysts, auditors, cybersecurity managers and threat analysts. Despite this, **educational institutions are slow to develop programmes that reflect the needs of the labour market.**

Another persistent problem is **the brain drain of experts and graduates abroad**. Students and graduates are increasingly leaving to study or work outside Slovakia, one reason being limited awareness of the quality of domestic higher education and of labour market needs, but also lower salaries compared to some EU countries. This trend is leading to a loss of professional potential in an area that is already facing a significant shortage of skilled workers. The number of qualified and high-quality teachers in the field of cybersecurity is low. It is desirable to strengthen coordinated lifelong learning for teachers in the field of cybersecurity, informatisation and digitalisation in cooperation with the Ministry of Education, Research, Development and Youth of the Slovak Republic.

Similarly, **only a limited number of institutions are active in the area of research**, although they nevertheless play an important role. Most research activities take place **at university faculties** and focus mainly on current technological trends such as artificial intelligence and PQC. Research in the field of cybersecurity is not systematically funded. Institutions rely primarily on external sources, such as European grant schemes or private sponsors. For the long-term sustainability and development of research, it is therefore essential to establish a stable national system for funding and coordinating research in the field of cybersecurity.

In addition to higher education, attention should also be paid to **secondary vocational schools or grammar schools**, which can prepare qualified workers for certain types of professions at this level. Expanding vocational programmes or adding vocational subjects could contribute to **a faster replenishment of the workforce** based on the needs of the labour market in the field of cybersecurity.

Strengthening the innovation environment is equally important. There are only a limited number of start-ups in the Slovak Republic focused exclusively on cybersecurity or the development of artificial intelligence solutions. U**niversity graduates and experts prefer employment** in the private or public sector **to setting up their own innovative projects** – start-ups. This situation is caused by the absence of a motivational system based on business support, but also, for example, the lack of specialised incubators and innovation hubs. These should function not only as on-site spaces, but also as platforms providing training, workshops, financing and grant support. The creation of such centres would significantly contribute to the development of an innovative environment and strengthen Slovakia's overall capacity in the field of cybersecurity.

IV. Policy and legal framework

Strategic and policy framework

Despite their non-legislative nature, strategic documents significantly influence policy-making and provide the basic framework needed to set cybersecurity priorities, anticipate future trends and regulatory requirements. These documents are produced at global, European and national levels and, although they are created individually, they often overlap and complement each other, contributing to a coordinated approach to cybersecurity. In the context of cybersecurity, the EU Cybersecurity Strategy for the Digital Decade and the Strategic Compass for Security and Defence are particularly important, as are the non-public intelligence and operational materials produced by the European External Action Service (EEAS).

The EU Cybersecurity Strategy for the Digital Decade represents the EU's approach to building a secure and resilient digital environment. It focuses in particular on **the resilience of critical infrastructure**, the development of technologies and capabilities, and the ability to prevent, detect and respond to large-scale cybersecurity incidents. The strategy also emphasises **achieving technological sovereignty** and deepening cooperation between Member States and institutions, thereby strengthening the EU's position as a global player in regulating responsible behaviour by states in cyberspace. These requirements are further elaborated in **the Strategy for the Resilience of Critical Entities of the Slovak Republic**, approved by Resolution No. 3 of the Government of the Slovak Republic on 9 January 2026.

The Strategic Compass for Security and Defence is one of the most comprehensive current documents on EU security and defence policy, setting out achievable goals for 2030. **It considers cyberspace to be a strategically important domain**, within which it defines a number of specific recommendations, particularly with regard to increasing capacities and strengthening cooperation on issues such as **shared situational awareness and rapid response to cybersecurity incidents**. Although both documents are predominantly political in nature, they play an important role in guiding national cybersecurity policies.

Binding legal framework

Unlike strategic documents, which set out political direction and long-term priorities, **EU legal acts define specific requirements for national authorities, critical sectors, digital products and emerging technologies**. Full implementation of these acts is essential not only for legal compliance but also for ensuring a coordinated approach to strengthening cyber resilience across the EU.

The National Strategy therefore directly takes into account the obligations arising from key legal acts, namely:

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Network and Information Security Agency) and on the certification of cybersecurity of information and communication technologies and repealing Regulation (EU) No 526/2013 (**Cybersecurity Act**), as amended

- Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing **the Digital Europe Programme** and repealing Decision (EU) 2015/2240, as amended

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules in the field of artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (**Artificial Intelligence Act**)

- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (**Cyber Resilience Act**)

The Cyber Resilience Act is European legislation aimed at increasing the security level of all products containing digital elements, with the exception of products covered by other EU regulations, such as medical devices, cars and similar technologies. The legislation applies to both hardware and software. The implementation of the Cyber Resilience Act into Slovak law will be carried out by a new law on cyber resilience, as well as by an amendment to Act No. 69/2018 Coll. on cybersecurity and amending certain laws, as amended, and Act No. 56/2018 Coll. on product conformity assessment, making a designated product available on the market and amending certain laws, as amended.

The practical implementation of the measures will lead to enhanced cybersecurity, as products with digital elements will only be allowed to be placed on the market after all known exploitable vulnerabilities have been removed. The manufacturer of these products is obliged to guarantee the same level of cyber resilience throughout the development and entire expected life cycle of the product. At the same time, products with digital elements are required to be delivered with settings that reduce the risk of vulnerabilities due to incorrect configuration. The regulation is designed in line with the concepts of "security by design" and "security by default".

» Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacity in the Union to detect, prepare for and respond to cyber threats and incidents, and amending Regulation (EU) 2021/694 (**Cyber Solidarity Act**)

» Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (**NIS 2 Directive**)

The NIS 2 Directive provides the basic legal framework for harmonising cybersecurity measures and tools with the aim of strengthening cyber resilience and security in the broader context of European integration and global threats.

NIS 2 expands the range of sectors and entities considered critical or important in terms of ensuring high cyber resilience, and modifies and clarifies the procedures for reporting cybersecurity incidents, the definitions of significant cyber threats, near-miss events and vulnerabilities, as well as incident response processes. The directive is also significant in that it defines a framework for strategic planning at national level, response to and resolution of large-scale cyber incidents and cyber crises. The Directive also strengthens international cooperation by establishing a European network of CSIRTs and a European network of cyber crisis liaison organisations (EU-CyCLONe).

» Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (**CER Directive**)

The CER Directive creates a new framework for strengthening the resilience of critical entities against physical, technical and natural threats. The CER Directive was transposed into Slovak law by Act No. 367/2024 Coll. on critical infrastructure and amending and supplementing certain acts (hereinafter referred to as the "Critical Infrastructure Act"), which contains measures to reduce the vulnerability and strengthen the resilience of critical entities operating critical infrastructure. The aim is to ensure the continuous provision of essential services that are key to maintaining the basic social functions and economic activities of the state. Transposition into Slovak legislation has led to a reorganisation of the competences of state administration bodies in the field of critical infrastructure, the introduction of new procedures for identifying critical entities and the obligations of the operators of these entities, as well as the introduction of requirements for the preparation of risk analyses, security plans and incident reporting, with an emphasis on the exchange of information between the Ministry of the Interior of the Slovak Republic as the central coordinating body, state authorities and the private sector.

These EU legal acts form the basic regulatory framework for cybersecurity in the Slovak Republic and define clear rules and tools for achieving the objectives of the National Strategy.

In the Slovak Republic, the basic legal framework for cybersecurity is formed **by Act No. 69/2018 Coll. on cybersecurity** and on amendments to certain acts, as amended, and amending certain acts (hereinafter referred to as the "Cyber Security Act"). Act No. 366/2024 Coll., amending Act No. 69/2018 Coll. on cybersecurity and amending certain laws, as amended, and amending certain laws, **Directive NIS 2 was successfully transposed into the legal order with effect from 1 January 2025**.

The new Cybersecurity Act **thus provides the legal basis for the development of a new National Strategy**. The National Strategy takes into account the requirements of Section 7 of the Cyber Security Act by providing clearly defined objectives and priorities in the field of cybersecurity. **The National Strategy, together with the Action Plan that will follow it, will define mechanisms for identifying relevant tools** and assessing risks, measures to ensure preparedness, the ability to respond to cyber threats and cybersecurity incidents, as well as subsequent recovery. The National Strategy also focuses on raising the general level of awareness of citizens and society on cybersecurity issues. At the same time, it promotes cooperation between the public and private sectors.

V. Vision of the National Strategy

The goal of every EU Member State is to **become a secure and trustworthy digital state** that supports the development and **safe use of innovative technologies.**

In line with European values, the principles of the rule of law, the protection of fundamental rights and freedoms, and ensuring the accessibility, openness and security of the internet will be promoted. It will also be important to support initiatives aimed at creating an open, fully democratic and rule-based cyber environment that respects international standards and the principles of proportionality and responsibility. The implementation of the National Strategy must therefore include **the systematic integration of cybersecurity into the digital transformation of the Slovak Republic.**

In the area of technological sovereignty, it is important to emphasise **the development** of **domestic research and development in the field of cybersecurity**. Supporting domestic start-ups, creating innovative ecosystems and utilising national talent are ways to reduce dependence on foreign suppliers and **increase digital sovereignty**. This sovereignty is also a driving force for innovation, and investment in research, testing environments and public-private partnerships will enable the rapid deployment of new solutions that improve service quality and support economic growth.

Building digital sovereignty should be based on the principle of technological neutrality. At the same time, the Slovak Republic must create a support system that will encourage research and development of information technologies, services and cybersecurity tools, and support participation in development projects and processes within the European Union. At the same time, it must support the deployment of such technologies in the Slovak cyberspace. Support and incentive mechanisms should take precedence over restrictive measures that could isolate the Slovak Republic from global technological progress or disrupt the open market.

An important element in building trust is **strengthening strategic communication and social resilience to disinformation operations**. Increasing citizens' media and digital literacy, transparent communication about security risks, and cooperation between the state and private companies contribute to public trust in digitalisation. User trust is a key prerequisite for the use of digital services, which is why it is essential to increase the transparency of digital solution providers, strengthen their responsibility for the security measures they put in place, and at the same time **improve citizens' awareness** of their role in **preventing cyber threats**. A digital environment in which citizens and organisations use online tools with confidence contributes to the prosperity of the state as a whole.

The growing complexity of the digital environment and increasing **cyber threats require innovative approaches to protecting data, systems and infrastructure**. Innovations in cybersecurity are key to sustainable resilience against cyber threats and also represent a strategic opportunity for the development of the knowledge-based economy. This objective supports the creation of a favourable environment for research, development and implementation of modern security technologies, while strengthening synergies between the state, academia and the private sector.

VI. Strategic pillars and objectives

Pillar 1: Protection of national cyberspace

OBJECTIVE 1.1: PROTECTION OF CITIZENS, SMALL AND MEDIUM-SIZED ENTREPRENEURS AND BUSINESSES

CURRENT STATE

State support for building cybersecurity awareness is not yet sufficiently systematic and unified, with responses to cyber threats often only occurring when a cybersecurity incident has already happened. Small and medium-sized enterprises do not always perceive cybersecurity as part of their responsible business practices and tend to view it as an additional financial burden to which they devote limited resources. As a result, they remain vulnerable to various types of cyber threats.

TARGET STATE

The goal is to create a secure environment while developing digital services so that they are perceived as a natural part of the everyday lives of citizens and businesses.

The resilience of the population, entrepreneurs and businesses to malicious activities in cyberspace **will increase** and the success rate of cyber attacks will decrease.

The state plays an active role in **raising awareness of cyber risks** and **provides simple instructions on how to protect** against them. At the same time, it supports the creation and **availability of tools to protect against cyber threats** that do not require a high level of technical expertise.

Prevention includes knowledge, methods and means to identify and protect **against harmful activities and false information created by artificial intelligence technologies**, which are becoming increasingly difficult to recognise.

The state supports **the cybersecurity community**, within which **the sharing of information and knowledge and cooperation** between civil society, the business sector and the state, are essential. Part of this system will be support for the participation of community centres, professional and interest organisations, and other non-governmental organisations in organising educational programmes, workshops, and the creation of competence and support centres. This will position the state not only as a respected authority but also as a trusted partner.

OBJECTIVE 1.2: CYBER RESILIENCE OF OPERATORS OF ESSENTIAL SERVICES

CURRENT STATE

Operators of essential services are not only state authorities and public authorities, but predominantly private companies. In many organisations, a gradual increase in the level of cybersecurity can be observed, but there are still cases where security does not even meet the basic required standards. The level of cyber protection depends primarily on the approach and willingness of the management of individual operators of essential services.

TARGET STATE

Security standards are defined at the national level and systematically implemented on the basis of a **professional risk analysis of the state and operators of essential services**. Operators of essential services implement and develop them in their business continuity plans in accordance with a centrally determined methodology and their own risk analysis, with an emphasis on strengthening cybersecurity and ensuring cyber resilience.

Highly critical or technologically specific sectors also effectively implement **specific security standards** based on legislation and good practice in the industry.

The state provides methodological support and actively supervises the fulfilment of obligations by operators of essential services.

The effectiveness of security mechanisms and measures to mitigate the impact of incidents **is regularly verified and adapted to current cyber threats** through regular testing, audits and reviews.

The cybersecurity system **interacts with the resilience of critical infrastructure**, including identified dependencies between individual sectors and organisations, causal links between the impacts of serious cybersecurity incidents, and an integrated response to serious and widespread cybersecurity incidents affecting critical entities.

The state actively **supports the deployment of such products and services** within information and communication technologies and operational technologies in the infrastructure of organisations and enterprises that guarantee **high cyber resilience**, in particular **products with security certification, cryptographic means resistant to known PQC threats, and similar technologies**.

At the same time, the state supervises **the responsible deployment** of technologies that may introduce new security risks into the information and communication technology and operational technology infrastructure of enterprises, **in particular artificial intelligence** and **networks of connected objects and devices** (the Internet of Things).

OBJECTIVE 1.3: SUPPLY CHAIN SECURITY

CURRENT STATE

Building a reliable and resilient supply chain is underestimated and consists only of contractual arrangements without the enforcement of additional measures. Companies that are part of supply chains are increasingly becoming the targets of attacks, due to the absence of systematic risk management and less effective implementation of security measures. At EU level, a Toolkit for the Security of the Supply Chain of Information and Communication Technology Services, Systems or Products has been developed, which defines the concepts of information and communication technology supply chain security, identifies potential risk scenarios and provides recommendations for addressing and minimising risks. It provides a common structured non-binding approach to securing the ICT supply chain and a general framework for conducting risk analysis of critical supply chains.

TARGET STATE

The state will ensure the implementation of a unified European framework for risk analysis and minimisation, enabling a common and **structured approach to the security of supply chains** for information and communication technology products and services.

As part of Europe's strategic direction, the state is **strengthening joint technological and strategic autonomy** by **diversifying partners** and **reducing dependence on risky suppliers**. This process is closely linked to the goal of building **secure, transparent and resilient supply chains** that support digital sovereignty and the credibility of the national technological environment.

Risks arising from supply chains will be **regularly assessed** and minimised by providers of critical basic services. High-risk suppliers of information and communication technology systems may be excluded from the operation of basic and important services or critical infrastructure.

A supply chain audit framework for critical sectors is in place.

Diversified and transparent supply chains will increase resilience and ensure the continuous operation of critical essential service operators.

Pillar 2: Building national cybersecurity capabilities

OBJECTIVE 2.1: INTEGRATED CYBERSECURITY GOVERNANCE ARCHITECTURE

CURRENT STATE

With the growing complexity of cyber threats, it is essential to build an integrated cybersecurity architecture. This architecture will ensure comprehensive protection of information systems, effective coordination and rapid response to cybersecurity incidents. The aim is to establish a centralised approach under the leadership of the National Security Authority and to build a situational awareness system that will enable the early detection and mitigation of cyber threats.

Information systems and digital services are currently fragmented, with varying levels of security and limited coordination between sectors. Not only cybersecurity, but also the level of digitalisation and the related information architecture suffer from a highly decentralised approach by the various responsible authorities and organisations. Although the National Security Authority plays a coordinating role, there is no unified situational awareness system or standardised crisis procedures at national level. The responsibility of sectoral authorities is often limited and coordination is mostly informal, which reduces the effectiveness of the response to cybersecurity incidents and cyber threats at national level.

Vulnerability management processes in public administration, as well as in some other entities, are either not implemented at all or are implemented ineffectively. Many entities only address vulnerabilities in response to a cybersecurity incident, which increases the likelihood of service disruption or data leakage. Operators of essential services often lack an overview of current vulnerabilities in the information technologies they use, as well as the mechanisms available to verify and eliminate them.

TARGET STATE

Cybersecurity management at the national level is integrated and systematically coordinated, so that individual entities and components and their activities together create **a functional system that is resilient to complex cyber threats**. Responsibility for cybersecurity is meaningfully distributed between **the National Security Authority, as the national authority and main guarantor of cybersecurity in the Slovak Republic**, and central government bodies, whether in the position of sectoral authorities or specific bodies responsible for cyber diplomacy, cyber defence or the fight against cybercrime.

The National Security Authority issues **methodologies and opinions** on the application of generally binding legal regulations and non-legislative documents in the field of cybersecurity.

Central authorities have **sufficient human, professional, financial and technical capacity to perform their tasks** so that the cyber resilience of the entrusted sector or the performance of the entrusted tasks is continuously improved.

The competences of individual authorities are clearly defined and delimited, while **transparent processes for mutual cooperation** and communication are established between them. These inter-ministerial processes ensure **effective outputs and procedures**, from the creation of rules and legislation, through response to cybersecurity incidents, to crisis management.

The public sector has an optimised and integrated cybersecurity architecture built on effectively managed IT architecture.

The cyber threat and cybersecurity incident detection system ensures the **timely detection of cyber threats across the entire cyberspace** in the Slovak Republic, thereby improving situational awareness. The **timeliness and targeting of warnings to relevant entities** is increasing.

A transparent **system for the fulfilment of tasks and responsibilities of all CSIRT units involved in preventive and reactive services** has been **adopted** and **implemented**, while the **procedure for escalating** cyber threats and cybersecurity incidents specified by the National Security Authority is **being followed**.

Vulnerability management is a normal part of the operation of networks, information systems and operational technologies. Vulnerability detection is carried out regularly and preventively. Operators of essential services have an **overview of available solutions** and actively use the support of CSIRT units in detecting and removing vulnerabilities, as well as in verifying the security level of their systems, thereby increasing the cyber resilience of the state and reducing the impact of potential cybersecurity incidents.

OBJECTIVE 2.2: EFFECTIVE IMPLEMENTATION OF SECURITY TECHNOLOGIES AND PROCESSES

CURRENT STATE

The use of innovative technologies is still in its elementary phase at the national level. Central government bodies in the field of cybersecurity are beginning to use artificial intelligence models in their activities, particularly in the analysis of large amounts of data, the processing of reports and, in some cases, detection activities. The use of artificial intelligence in these areas is still at an early stage. Organisations are unaware of the risks and, by introducing new technologies, are creating new vulnerabilities and even incidents. At the organisational level, there are no internal methodologies for working safely with artificial intelligence.

TARGET STATE

Central government bodies, operators of essential services, CSIRT units and other relevant entities are able **to use AI-based models and tools** to improve their information infrastructure and processes, **including security technologies**. These tools are used not only as **automated detection tools for the rapid identification of cyber threats** and cybersecurity **incidents**, but also for the rapid search and **analysis of relevant information from open sources**, the analysis of large amounts of data, for example, **in forensic analysis and simulations**.

Security monitoring centres will rely on **technologies and mechanisms** that ensure continuous and **timely detection of incidents**, exchange and **analysis of threat data**, measurement of their occurrence, and proactive general or targeted warnings about them to build situational awareness. Overall **situational awareness** at the national level will **be ensured by automated tools, including the use of artificial intelligence** and effective processes, so that the response to threats and incidents is immediate and adequate.

OBJECTIVE 2.3: RESPONSE TO CYBERSECURITY INCIDENTS, CYBER CRISES, AND COOPERATION WITH JUDICIAL AUTHORITIES

CURRENT STATE

An effective response to cybersecurity incidents is the basis of a functional cybersecurity system. The cybersecurity incident response system is functional at the national level, but there are shortcomings in the coordination between CSIRTs and the national CSIRT (SK-CERT). The capacities of CSIRT units are insufficient, and the detection, reporting and resolution of cybersecurity incidents often depends solely on specific situations and individual decisions. There are no internal manuals in place regarding the severity or scope of a cybersecurity incident. The process of resolving cybersecurity incidents is lengthy due to organisational, technical and human factors. The police and judicial authorities are not adapted and equipped to effectively detect and investigate cybercrime. Differences in procedures for obtaining and securing digital evidence persist, due to factors such as varying national legislation, technological complexity, the problem of territoriality, complicated jurisdiction, the lack of uniform European standards for tools and methodologies used to obtain, secure, analyse and store digital evidence, and the lack of specialised training for the police and judicial authorities. The police and the public prosecutor's office face a shortage of experts, technical resources and knowledge to investigate computer crimes. Exercises to simulate attacks and responses to them are not organised frequently enough, and the implementation of the conclusions of the exercises cannot be verified, which reduces preparedness for crisis situations. With the development of information and communication technologies, there has been an increase in intolerance in cyberspace. Children are a particularly vulnerable group, as they are often exposed to disinformation and cyber threats.

TARGET STATE

This objective supports the development of the capacities of CSIRT units and security forces, the introduction of regular exercises to increase preparedness, and the implementation of education in the field of cyberbullying.

The integrated cybersecurity incident response system (the "national blueprint") includes the national CSIRT (SK-CERT) and networks of sectoral and other CSIRTs covering public authorities and other important sectors. The functionalities of the Unified cybersecurity system are used for coordinated procedures in dealing with serious cybersecurity incidents. **Clear procedures** and competences of individual components **are defined** for **dealing with large-scale cybersecurity incidents and cyber crises**, ensuring a rapid and coordinated response. These procedures are regularly reviewed. The national blueprint will also be linked to the European cyber crisis management mechanism (the EU blueprint).

Operators of essential services are sufficiently **prepared to deal with serious cyber incidents**. The ability to respond to cybersecurity incidents is strengthened so that timely intervention prevents more widespread impact.

Cooperation **between the police, the public prosecutor's office and the judicial authorities** ensures **the effective detection and investigation of cybercrime** with a view to bringing perpetrators to justice, including the fight against cyberterrorism and cyberespionage. The judicial authorities **use established expert units, specialists and experts** to effectively investigate cybercrime. At the same time, **they communicate and cooperate effectively with the judicial authorities of other countries** within and outside the EU.

In the fight against cybercrime, **changes** have been made to the national legal framework **to enable criminal liability to be established** in relation to **cyberterrorism or cyber espionage** threats, including on the basis of secure **electronic evidence**. An effective system for prosecuting the most serious forms of cybercrime has been put in place, while adequate legal protection is provided to investigators, with information and evidence obtained during investigations protected from misuse.

The police force has **reinforced** its **specialised units** to combat crimes committed in cyberspace. In the digital dimension, the state has **also strengthened the protection** of intellectual property and protection **against industrial and technological espionage**, especially in the field of new and breakthrough technologies, but particularly those that have applications in the area of national security and defence.

Education has been introduced for pupils, teachers, educational advisers, other cooperating experts, non-teaching staff and parents on the issues of **disinformation, cyber threats and their prevention**.

Rapid response to cybersecurity incidents and effective and decisive accountability of threat actors at the criminal or diplomatic level must act to reduce the motivation to carry out malicious activities or commit cybercrime.

Pillar 3: Secure and innovative digital products and services

OBJECTIVE 3.1: ENSURING CYBERSECURITY THROUGHOUT THE LIFECYCLE OF DIGITAL PRODUCTS AND SERVICES

CURRENT STATE

Cybersecurity is perceived as an additional element rather than an integral part of the development and management of digital solutions. In its current state, it does not fully reflect technological trends, in particular the deployment and use of artificial intelligence models.

TARGET STATE

This objective aims to create regulatory, procedural and technical conditions that will ensure that products and services are secure from their inception and throughout their lifetime.

The development of technology companies is key to building an advanced economy and digital sovereignty. The system of direct and indirect support, regulation and security certification is designed to ensure that technology companies are competitive and motivated **to develop and provide modern and highly secure digital products and services**. These are designed in accordance with the principles of **"security-by-design"** and **"privacy-by-design"**. All phases of their life cycle include **security requirements as fundamental characteristics of the product** or service. A suitably chosen risk management methodology also reflects the introduction of artificial intelligence into digital products and services, identifying and assessing new risks associated with it (e.g. cyber threat modelling).

Digital products and services are developed and marketed in **accordance with the requirements of the Cyber Resilience Act, the Artificial Intelligence Act and other legislative requirements**. Their manufacturers and providers apply appropriate security requirements throughout the entire life cycle, adhere to secure development principles, maintain and share a software bill of materials (SBOM), perform security testing, operate effective vulnerability detection and remediation processes, and fulfil reporting obligations.

The processes for detecting and **responsibly reporting vulnerabilities** are clearly defined and effectively implemented. The risk associated with not only networks and information systems but also digital products are reduced. Digital products based on **artificial intelligence technologies** meet regulatory requirements as well as **ethical and security standards recognised in the industry**.

OBJECTIVE 3.2: INTRODUCTION OF SECURE DIGITAL PRODUCTS, SERVICES AND INNOVATIONS

CURRENT STATE

Platforms and software are often selected without thorough consideration of the risks involved, vulnerabilities are only discovered after deployment, and the complexity of interconnected systems makes comprehensive risk analysis difficult. At the same time, horizontal rules for digital products and systems (Cyber Resilience Act, Artificial Intelligence Act) are coming into force in the EU, introducing obligations for secure development, vulnerability management, transparency, risk management and conformity assessment throughout the entire life cycle. In parallel, the area of certification of persons, products, processes and services is developing, but a comprehensive portfolio of schemes is still lacking, the number of accredited bodies (especially for products) is low and the demand for certification is limited.

TARGET STATE

New technologies, information systems, digital products and services are marketed, procured or **implemented according to the principles of "security-by-default"** with systematic vulnerability testing, protection against common attack vectors and the application of zero-trust approaches (access control, segmentation).

When introducing new technologies, organisations **take into account the requirements for high resilience to cyber threats** and do not prioritise functional requirements over cybersecurity requirements. Certified products and services are primarily procured.

An **effective security certification system** based on European certification frameworks is in place. The state has functional certification capacities recognised at European level.

Manufacturers are aware of the need to certify their products and services. The **number of European certification schemes** for products, processes and services incorporated into the Slovak certification framework has increased. **Manufacturers of digital products** and services naturally consider **security certification to be a market advantage**. The requirements of the Cyber Resilience Act, the Artificial Intelligence Act and the requirements for security certification are appropriately integrated into public procurement criteria and contractual conditions.

Providers and **integrators of artificial intelligence technologies implement risk management**, ensure data quality, documentation, transparency and human oversight, with high-risk systems undergoing conformity assessment.

The number of accredited and notified conformity assessment bodies has increased, ensuring a healthy competitive environment.

Pillar 4: Education, skills and awareness

OBJECTIVE 4.1: BUILDING NATIONAL KNOWLEDGE CAPACITY AND EDUCATION

CURRENT STATE

Supporting cooperation between public administration, the private sector and academia, as well as introducing systematic education across all levels of education, is key to strengthening the national cybersecurity system. An important element is the creation of conditions for the development and certification of cybersecurity experts, which will contribute to increasing the expertise and sustainability of the entire system. Particular attention should be paid to building the knowledge and capacity in specific areas of the Internet of Things, artificial intelligence and PQC. There is a shortage of qualified cybersecurity experts in the Slovak Republic, which is a consequence of the absence of systematic education in this area at all levels of the school system. Cybersecurity is not sufficiently integrated into the school curriculum, and there is a lack of comprehensive training for teachers who would be able to cover the topic effectively. The range of specialist study programmes is not sufficiently developed, responds poorly to the needs of the labour market, and there is also a lack of national certification mechanisms for verifying expertise in the field of cybersecurity.

TARGET STATE

Cybersecurity is **an integral part of educational programmes at all levels of education**, ensuring the long-term preparedness of human resources for the new challenges of the digital environment. There is an effective system for training experts, certification and support for innovative research, with an emphasis on building awareness from the lowest levels of education.

A comprehensive and coordinated cybersecurity education system has been established to support the development of professional capacities at all levels of education. **Primary and secondary schools** systematically **develop awareness and habits** in the field of cybersecurity and digital skills. **Universities** and professional institutions ensure **the training of qualified experts** across professions.

Cooperation between educational institutions is strengthened, with an expanded **range of accredited programmes** and a **system of lifelong learning** and professional training in place. A **specialised type of education** is created **for specific sectors** to strengthen competencies and sustainably build human capital in the field of cybersecurity. The environment will enable the continuous development of competences and the sustainable building of human capital in the field of cybersecurity.

The Cyber Security Competence and Certification Centre, as well as other competence or support centres at the level of other central government bodies and universities, play an important role in building the knowledge base and professional human capacity. The National Coordination Centre acts as a platform whose main objective is to build and support the professional community and share information, actively organising and supporting professional conferences, seminars, workshops and training courses.

The knowledge-capacity framework is complemented by **scientific and research centres focusing on applied cybersecurity**, including the development and deployment of artificial intelligence.

Partnerships with the private sector and academia are systematically established to promote the sharing of knowledge, information and best practices, and to deliver innovative solutions for the cyber resilience of the state.

CIEĽ 4.2: ZVYŠOVANIE DIGITÁLNEJ GRAMOTNOSTI OBČANOV A BEZPEČNOSTNÉHO POVEDOMIA

CURRENT STATE

The development of digital literacy and public awareness is a fundamental prerequisite for building a society that is resilient to cyber threats and manipulative techniques. In the era of artificial intelligence and increasing digitalisation, it is essential that citizens have the knowledge and skills necessary to use technology safely and responsibly. It can be said that the general public still has a low level of digital literacy and awareness of the risks associated with the use of information and communication technologies. Citizens are often unaware of the principles of safe behaviour in the online environment, such as personal data protection, secure use of passwords, or verification of the accuracy of information. Knowledge of how artificial intelligence and algorithms work and their impact on everyday life is limited. There is also a lack of awareness of new threats, such as disinformation created through artificial intelligence or cyber fraud based on social engineering. Although digital security education is partly provided through school programmes, there is no systematic and long-term approach covering all age and social groups of the population.

TARGET STATE

The goal is to create an informed society that can use critical thinking to recognise the risks of the digital environment, assess their credibility and effectively prevent them.

Society in the Slovak Republic achieves **a high level of digital literacy**. Citizens know and apply the basic principles of safe behaviour in the online environment, are **aware of the risks associated with the use of modern technologies** and are able to actively protect themselves against them. Basic knowledge of cybersecurity, hybrid threats, artificial intelligence and its ethical, legal and social implications is a natural part of general education. Systematic protection of children, pupils and young people in cyberspace is ensured.

People are able to **recognise content created by artificial intelligence** and critically evaluate the information they receive. The education system and public administration institutions support the development of skills for the safe and ethical use of new technologies. The development and deployment of methodologies, guidelines and procedures for detecting false content and other manipulative techniques is supported.

The introduction of artificial intelligence into the educational process and the digital environment is accompanied by **specific security and ethical measures** that take into account their protection against unauthorised manipulation, disinformation, data misuse and other cyber threats.

A basic understanding of digital skills and cybersecurity is **part of the general knowledge of society as a whole**. It is **included in the general curriculum** of primary and secondary schools as part of compulsory subjects. At the same time, programmes, courses, seminars and other lifelong learning tools aimed at all age groups are supported, as is close cooperation with the private sector in this regard.

The National Security Authority supports the targeted and systematic digitisation of public services and their secure use at the national level.

Pillar 5: Strategic partnerships and international cooperation

OBJECTIVE 5.1: EFFECTIVE INTERNATIONAL COOPERATION

CURRENT STATE

The Slovak Republic systematically builds and maintains **partnerships in the field of cybersecurity and cyber defence** within major international organisations (EU, NATO, UN, OSCE, Council of Europe) and through bilateral agreements. It participates in initiatives that contribute to strengthening global cyber resilience. The Slovak Republic is actively involved in ENISA activities. The Slovak Republic also plays an important role in the NATO Cooperative Cyber Defence Centre of Excellence. The Slovak Republic is an integral part of the European and transatlantic area based on democracy, the rule of law and the protection of fundamental rights. The EU and NATO provide a strategic, technological and security framework for joint projects, information exchange and coordination of responses to cybersecurity incidents. The Slovak Republic is also strengthening its ties with, and contribution to, the OSCE and the UN, which shape international standards and policies in the cyber domain. Experience to date confirms the importance of regional cooperation, particularly within the V4, for information exchange, sharing of best practices and coordination in cross-border incidents. The national CSIRT unit (SK-CERT), which is part of the National Cyber Security Centre, is a member of the European network of national CSIRT units. Several Slovak CSIRT units are involved in international communities and joint exercises.

TARGET STATE

The state continues to be a **trusted, respected and integrated partner within the EU, NATO, the UN, the OSCE and relevant regional groupings**, with clearly defined roles, contact points and processes for day-to-day cooperation and coordination in crisis situations. The Slovak Republic effectively uses channels for sharing information, coordinating responses and joint interventions in cross-border cybersecurity incidents, while **regularly participating in** ENISA, NATO and other international exercises with demonstrable improvements in interoperability.

The Slovak Republic is also **building and developing the concept of cyber and digital diplomacy**, including the appropriate application of standards of responsible behaviour in global cyberspace and compliance with the principles of international law. In close cooperation between the Ministry of Foreign and European Affairs of the Slovak Republic and other relevant authorities, the Slovak Republic is actively involved in international organisations and global and European forums that shape norms, standards and policies in the field of cybersecurity with the aim of increasing the diplomatic engagement of the Slovak Republic, strengthening its visibility and building its image as a modern and secure country, and contributing to the creation of an international environment based on **responsible behaviour by states in cyberspace**.

At the regional level, it is a responsible partner in coordinating preparedness, rapid alerts and strategic communication during major incidents. The Slovak Republic also ensures the full application of the Cyber Diplomacy Toolkit as a mechanism for preventing and deterring harmful cyber activities and will actively cooperate on attribution modalities with EU Member States and strategic partners from third countries.

In line with EEAS recommendations and current international trends, a fully established organisational unit led by a specially appointed ambassador has been created at national level to address issues of cyber and digital diplomacy and technology. This unit will enable Slovakia's full integration into the relevant international structures in the EU, UN, OSCE, Council of Europe and other diplomatic technology platforms.

The Slovak Republic actively participates in activating **the European cyber** solidarity **mechanism**, which aims to help other affected EU Member States and candidate countries respond to large-scale cybersecurity incidents. In this regard, the Slovak Republic also contributes its expertise and information to ensure and increase the resilience of the EU as a whole.

In solidarity with partners within under attack within the EU and NATO, it participates **joint attribution processes**. This mechanism is a continuation of the activities and objectives that were initiated under the previous strategy. **As part of cyber diplomacy**, an **effective attribution mechanism has been put in place** to strengthen the capacity for **diplomatic response** to cybersecurity incidents, either individually or in cooperation with trusted partners.

In order to ensure its own national security in cyberspace, the Slovak Republic **attributes cyber attacks. Attributing attackers** is a very demanding process that requires sufficient human resources and well-established processes. The state is strengthening its analytical capacities in the area of security threats, specialising in the attribution of cybersecurity incidents. A well-established process of technical and political attribution of cybersecurity incidents is complemented by legal mechanisms and cyber diplomacy mechanisms.

The Slovak Republic participates **in European cyber solidarity mechanisms**, which aim to aggregate and utilise the joint capacities of Member States in responding to large-scale cybersecurity incidents and cyber crises. At the regional level, it plays a leading role within the V4 in coordinating preparedness, rapid alerts and strategic communication during large-scale cybersecurity incidents.

In the field of artificial intelligence, the state applies and harmonises **standards for the safe and ethical use of artificial intelligence** (risk management, auditability, responsible deployment) that protect fundamental rights and increase the resilience of critical infrastructure. These standards are implemented in practice through joint programmes, exercises and research projects with allies.

VII. Implementation framework

In order to successfully achieve the strategic objectives, set out in the National Strategy, it is necessary to create a comprehensive Action Plan for the Implementation of the National Cybersecurity Strategy for 2026-2030 (hereinafter referred to as the "Action Plan"), which clearly defines the tasks, timetable, responsibilities and measurable implementation indicators (KPIs) so that the process of achieving the strategic objectives is effective and controllable. The Action Plan must be consistent with the priorities of the strategy and at the same time flexible enough to respond to trends, changing conditions and the needs of society.

Given the rapid pace of development in information and communication technologies and other emerging technologies, the Action Plan must also be capable of being updated during the implementation period if required by circumstances.

After adopting the National Strategy, the Slovak Republic shall notify the European Commission of the National Strategy within three months of its adoption.

Action Plan

The Action Plan for the implementation of the National Strategy shall specify:

- specific tasks divided according to strategic objectives, together with individual steps
- the responsible entities in the role of coordinators and participating entities,
- the manner of implementation of individual tasks and activities and the impacts or estimated costs incurred by individual tasks,
- the time frame for completing the tasks.

The National Security Authority is responsible for drawing up the Action Plan, involving all interested parties in its preparation.

The proposed measures will be based on an analysis of the environment, risks and needs of the entity, with funding coming from its own budgets, programmes and projects, inter-ministerial programmes and shared EU resources. The EU offers a wide range of funding opportunities for cybersecurity projects. In addition to the better-known euro funds, there are also so-called directly managed EU programmes through which Brussels directly announces calls for project funding. Examples of such programmes are Digital Europe and Horizon Europe. The National Security Authority will provide methodological assistance with the submission of projects. However, the proposed measures will not, beyond the obligations laid down in generally binding legal regulations, burden business entities that have been designated as operators of essential services or as operators of critical essential services.

Stakeholders

The main stakeholders in the cybersecurity system of the Slovak Republic who will participate in the implementation of the objectives of this National Strategy include, in particular:

- The General Prosecutor's Office of the Slovak Republic
- Cyber Security Competence and Certification Centre,
- Ministry of Transport of the Slovak Republic,
- Ministry of Finance of the Slovak Republic,
- Ministry of Investment, Regional Development and Informatisation of the Slovak Republic,
- Ministry of Defence of the Slovak Republic,
- Ministry of Justice of the Slovak Republic,
- Ministry of Education, Research, Development and Youth of the Slovak Republic,
- Ministry of the Interior of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic,
- Ministry of Health of the Slovak Republic,
- Presidium of the Police Force,
- Slovak Information Service,
- Office for Personal Data Protection of the Slovak Republic,
- Office of the Government of the Slovak Republic,
- Military Intelligence,
- operators of essential services,
- universities and other educational institutions,
- representatives of companies, entrepreneurs and operators of essential services from the private sector.

Cybersecurity is directly related to or closely interacts with other areas of law and public administration. These are primarily areas related to:

» the informatization and digitalisation of public administration,

» the protection of critical infrastructure,

» state crisis management,

» state defence,

» personal data protection,

» data interoperability, and

» regulation of artificial intelligence.

Emphasis will be placed on regular mutual communication, information exchange, process interoperability and consistency of recommendations so that cybersecurity measures naturally complement measures in other areas.

The key partners of the National Security Authority are central government bodies (ministries, other central government bodies) and government bodies with nationwide jurisdiction (e.g. the Office for Personal Data Protection of the Slovak Republic).

Coordination and cooperation between these central government bodies will be ensured by setting up cross-cutting or thematic working groups that will link expertise between cybersecurity and other areas. The working groups will thus create a single space for coordinating planning, methodological approaches and information exchange between the above-mentioned central authorities and other ministries, regulators and public institutions. Emphasis will be placed on regular mutual communication, process interoperability and consistency of recommendations so that cybersecurity measures naturally complement measures in other areas.

In the field of artificial intelligence, it will be necessary to consistently implement the EU regulatory framework and build an institutional basis for regulating the development, deployment, use and security of artificial intelligence in the Slovak Republic. The expected legislation will set out the division of competences and tasks of the individual central government bodies that will carry out regulation and state supervision.

Monitoring Committee

The Monitoring Committee for the implementation of tasks arising from the Action Plan (hereinafter referred to as the "Monitoring Committee") will play a key role in the implementation process. The Monitoring Committee will be established and composed of representatives of those state authorities whose representatives are mandatory members of the Cyber Security Committee of the Security Council of the Slovak Republic, which is a working body of the Security Council of the Slovak Republic.

The task of the Monitoring Committee will be to coordinate cooperation between the various stakeholders, monitor the progress of the Action Plan tasks, identify any problems and propose solutions. At the same time, it will serve as an important platform for the exchange of information, expert dialogue and ensuring the transparency of the entire implementation process. Its active role is one of the pillars of the successful fulfilment of the strategic objectives in the field of cybersecurity in the Slovak Republic.

Financing

In order for the Slovak Republic to be able to fulfil its objectives and achieve results, it is necessary to ensure adequate access to sufficient financial resources from both public and private sources. In this regard, the possibilities of financing from the state budget, shared EU resources, such as cohesion policy programmes, as well as so-called directly managed funds come to the fore. Cybersecurity must not be left out when programming national objectives or opening up opportunities for co-financing with private capital. The correct setting of the future multiannual financial framework for 2028-2034 will be particularly important.

Each of the relevant entities involved in the implementation of the National Strategy objectives and tasks to be set out in the related Action Plan will be responsible for ensuring adequate funding for these tasks and activities.

VIII. Conclusion

The National Strategy represents a strategic plan and a commitment by the state to protect and strengthen the digital environment as an integral part of national security, economic stability and the protection of democratic values. The successful implementation of the strategy will depend on the ability of all stakeholders to act in a coordinated manner, share information, implement best practices and respond flexibly to dynamically changing threats.

Equally important will be the ability to continuously invest in prevention, research, education and innovation so that the Slovak Republic can maintain and strengthen its resilience to cyber threats and cybersecurity incidents. The National Strategy expresses the Slovak Republic's commitment to ensuring the integrity, availability and confidentiality of digital services and infrastructure, strengthening cooperation with allies and partners, promoting the principles of an open, free, stable and secure cyberspace, increasing digital literacy and security awareness among the population, and supporting technological innovation in line with European values. The National Strategy also addresses the prevention and prosecution of cybercrime, as well as the capacity to counter a broad range of malicious activities in cyberspace.

The implementation of the measures defined in this National Strategy will be carried out in accordance with the legal framework of the European Union, the generally binding legal regulations of the Slovak Republic, as well as relevant international commitments. This approach will ensure the creation of a secure digital environment that will support economic growth, increase citizens' confidence in digitalisation and protect national interests.