NATIONAL SECURITY AUTHORITY

SK NBÚ CERT

THE NATIONAL CYBERSECURITY STRATEGY 2021 - 2025

Table of Contents

Foreword

Hardly any area in the modern world is evolving as quickly as the challenges posed by the state's cybersecurity governance. A thorough setting of processes, procedures and objectives needs to be fully adapted to the dynamics of this trend.

A new National Cybersecurity Strategy is emerging at a time when it may seem too late for taking many measures. Various attackers make great strides every day. It is possible that even at this moment anyone can be a target of a cyberattack without realizing it.

The state and its critical infrastructure have been a target of both state and non-state actors for a long period. Today, cybersecurity incidents are often sophisticated and creative. Approach to them should be exactly the same. The intention of the National Cybersecurity Strategy for the years 2021-2025 is simple – to prepare and bring Slovakia to the level at which it is always one step ahead of a potential threat.

Each of us wants a modern, digitized country in which instead of standing in rows, we can arrange comfortably everything from our home or office. However, the comfort of modern conveniences requires even greater vigilance. The document names the principles on which the strategy of the Slovak Republic is based, identifies cyberspace threats and clearly defines the objectives or directions that the country must take in protecting not only the virtual world.

The vision of the National Security Authority is to strengthen and create an open, free and secure cyberspace for everybody.

A precondition for success in collective security is in particular a common interaction. Each entity is only as strong as its weakest element. Any strategy is essentially intended to unite individuals into groups, groups into organisations and organisations into a system with a common objective.

The National Cyber Security Strategy, elaborated by the National Security Authority, is therefore intended for anyone involved in any way in building a cybersecurity governance system of the Slovak Republic. It is and will be the umbrella document on which the basic direction of the country in this field is based.

Roman Konečný

Director of the National Security Authority

1. Introduction

The modernization of society through information and communication technologies, its digitalization and the development of innovative services is an undeniable fact that has become a natural part of our lives. Nevertheless, the development that comes with expansion of opportunities must be balanced by responsibility for the risks that emerge simultaneously as a forfeit for the benefits of the digital society.

Cybersecurity is a state in which information systems and services are resilient to current threats and vulnerabilities, and ready to detect and handle cybersecurity incidents, recover data and processes, and minimize consequences. Nonetheless, cybersecurity is not an issue concerning only particular organizations and entities that protect their assets by taking appropriate measures.

Informatization of the public sector, automation of manufacturing and other processes that were performed manually in the past, constant development and easy availability of technologies, their ease of use in a wide range of common activities create a space in which, apart from undeniable advantages, threats arise, targeting critical and sensitive systems and services of the state. They can result in a breach of citizen's trust in the government, cause extensive financial and economic damages, and potentially cause injuries or a loss of life.

The information and cybersecurity governance system, the goal of which is to ensure a high degree of resilience of systems and services as well as effective detection and response capabilities, is a strategic security interest of the Slovak Republic. A comprehensive concept of information and cybersecurity governance, strategic direction based on clear principles and exactly defined strategic objectives are the basis for a well-developed system that can flexibly respond to current threats and ensure a high level of cybersecurity at national level. This is the concept of the National Cybersecurity Strategy for the years 2021 - 2025.

The history shows that the National Cybersecurity Strategy for the years 2021-2025 (hereinafter referred to as the „National Strategy") is not the first strategic document created at the national level. In 2007, a strategy of information security was created together with an action plan, and subsequently the Cyber Security Concept of the Slovak Republic for 2015-2020 (hereinafter referred to as the „Concept") was introduced, which was the first comprehensive plan defining the cybersecurity principles, rules and objectives. The measures framing the Concept focused on creating an institutional framework for governance, adopting appropriate legislation, developing basic mechanisms for cyberspace governance, developing an education system, creating a risk management culture, active international collaboration and supporting science and research. Along with the Concept, the Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020 (hereinafter referred to as the „Action Plan") was created, defining specific tasks related to individual measures, entities in charge and responsibilities of participating bodies, as well as the time frame for the task completion. Within the time period defined for the Concept and the Action Plan, it was possible to create a stable institutional framework for cybersecurity governance, adopt a historically first comprehensive legislation in the field of cybersecurity and to create specialized entities for cybersecurity incident handling.

Cyber threats as well as cybersecurity are constantly evolving. New targets and vectors of cyberattacks are constantly emerging, and are becoming more widespread, more frequent and more sophisticated. Some states and non-state actors resort more and more to pursuing their goals through unfair cyber activities. These can take several forms, including critical infrastructure attacks, cyber espionage, intellectual property theft, cybercrime, and cyberattacks as part of hybrid threats. Cyberspace is increasingly becoming an area of strategic confrontation among states, reflecting a dynamic geopolitical environment and efforts to change the current international order. Technological innovations, including cybersecurity innovations, are becoming an instrument of confrontation and growing tensions in the political, economic and security fields.

The good news is that the strategic direction of the cybersecurity system can build upon the solid foundations laid by the Concept and developed by its Action Plan, even though some of the goals have not yet been achieved.

The new strategy expands on the previously carried out activities and its ambition is to respond in a modern way to current and future security threats, define the principles of the cybersecurity system and to determine strategic objectives, the achievement of which will ensure a higher level of security in the cyberspace of the Slovak Republic. The National Strategy is intended for all entities that participate in building the cybersecurity system of the Slovak Republic and is a key document from which the basic direction of the Slovak Republic in this area comes from.

The vision of the National Strategy is to strengthen and create an open, free and secure cyberspace for everybody.

2. Principles

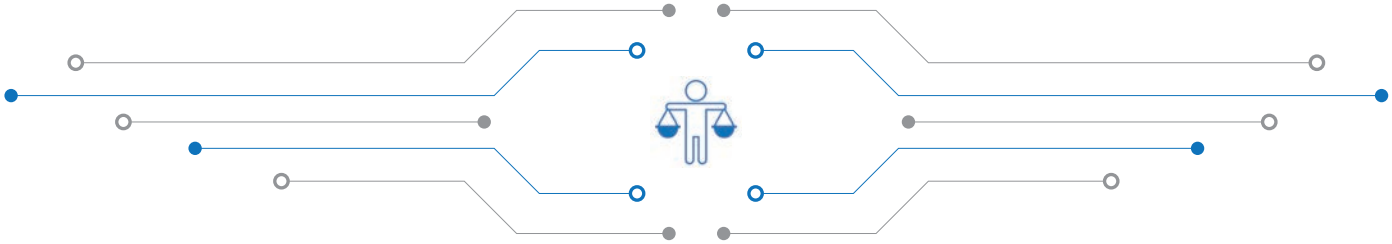
> Cybersecurity of the Slovak Republic is addressed by a complex system that includes not only regulations but also practical activities, such as risk management, detection and cybersecurity incident handling, system recovery, education, dissemination of security awareness and, last but not least, research and development of cybersecurity tools and processes. In order for such a large-scale system to work and for the various stakeholders to work together to maintain and develop it, the fundamental principles, based on the democratic values of the rule of law and reflecting a modern approach to national cybersecurity and international cooperation in this field, must be respected.

2.1 Fundamental human rights and freedoms come first in cyberspace

Cyberspace is a place where an increasing number of users meet with the ongoing digitalization, where they not only realize their needs, but also pass on part of their identity and privacy. We use the Internet for communication with our families and friends, purchase of consumer goods, paying bills or for managing our smart homes. Cyberspace is also a special operational domain, recognized by the North Atlantic Treaty Organization.

Like the physical world, the cyberspace is not an ideal place as well. In the last two decades, we have witnessed an increasing frequency of cyberattacks, greater sophistication of attackers and increasing losses on the part of victims. The Slovak Republic promises to respect fundamental human rights as defined in the Universal Declaration of Human Rights and promotes the position that human rights are enforceable both in the „offline" and in the „online" space. The Slovak Republic upholds and enforces this position in the long term and commits to other states with the same value system, and also supports the responsible behavior of states and a uniform interpretation of international law in cyberspace.

We have to consider the cyberspace as the equivalent of the physical world, together with the application of clear rules that will respect the fundamental human rights and freedoms stipulated by the constitution, including the right to privacy, so that it is not only secure but also open, free and accessible to everybody concerned. The security of cyberspace must be interconnected to its freedom, and fundamental human rights and freedoms in the digital space can only be guaranteed if the digital sovereignty of the states of the European Union as a whole is preserved, which also ensures the independence and sovereignty in cyberspace.



2.2 Cybersecurity governance system based on legality and mechanisms of the security system of the Slovak Republic

The Slovak Republic is a country governed by democratic values ensuring the rule of law. The cybersecurity governance system therefore respects the principles that are inherent in the Slovak Republic and which create an environment where the laws, rights and freedoms of citizens are respected. The cybersecurity governance system fully respects the Constitution of the Slovak Republic and the applicable and effective laws, while also relying on the Government's Policy Statement in the strategic objectives and tasks of the National Strategy.

The National Strategy has a legal basis in Act No. 69/2018 Coll. on Cybersecurity and on Amendments and Supplements to certain Acts (hereinafter referred to as the „Act" or „Act on Cybersecurity") and reflects the mandatory content enshrined in Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union and has been transposed into this Act. It also reflects the strategic direction in the field of security and observes the principles enshrined in the Security Strategy of the Slovak Republic.

2.3 Comprehensive (universal) approach to cybersecurity issue

There is no universal guide to ensure the security of cyberspace. It is a continuous process that must react to many complex aspects. At the same time, it is necessary to remember that the technological progress of society and modern technologies that penetrate our lives are developed much faster than the rules of their safe use.

The cybersecurity issue needs to be addressed in such a way that its solution is reliable, comprehensible and understandable. It is not sufficient to develop individual cybersecurity components, but there must be clear relation between these components, forming a functional system. Cybersecurity is not a stand-alone entity. It is important to understand that ensuring a high level of cybersecurity is a means of successful socio-economic development of society and enhancement of the state's resilience to security threats. An integrated link of cybersecurity to other sectors, and understanding of interactions between security and the functioning of society constitute an essential component of the rationale and importance of addressing the cybersecurity at national level.

Cybersecurity and information security are dedicated to the protection of information assets. Information security addresses the security of assets regardless of where and how the information is processed, and cybersecurity deals with the security of only a certain part of information assets, namely those processed in virtual space. Data will become information when they acquire some significance, meaning, and mainly the value. In this context, both cybersecurity and information security ensure the security of any information, including personal data. The overlap of cybersecurity and information security with the protection of personal data is the achievement of their objective – the protection of any data and information.

2.4 Risk management as a key element of the national cybersecurity governance system

Cybersecurity measures must always be proportionate and balanced to the risk they are designed to mitigate. Risk analysis is an essential activity to determine the current status of assets and threats, vulnerabilities, severity of risks and potential impacts. Such analysis results in a quantitative or qualitative assessment of current risks and consequently, it is possible to identify precisely the measures to mitigate these risks.

The cybersecurity governance system at both national and sectoral levels is based on the risk management approach, as a comprehensive and precise method for identifying risks at different levels of cybersecurity governance. Risk identification at different levels will allow making decisions on targeted and effective measures that will not incur disproportionate costs and will identify specific steps to be taken to achieve a high level of cyberspace security.

2.5 Support, cooperation and prevention

Cybersecurity must be understood as a common interest of the state, its citizens, commercial and non-commercial organisations. Therefore, it is necessary to create rules in the form of laws, regulations, methodologies and technical standards, but at the same time, it is necessary to create these rules so that they are truly enforceable.

Given the nature of the cybersecurity system and its complexity, it must be the interest of the state to support respective involved entities in taking the necessary measures, to cooperate with them on creating rules and standards, as well as to educate these entities sufficiently and to share experience with them. The state through its support and cooperation makes efforts to build a mutual trust of involved entities. Repression and sanctions must be a means of „ultima ratio", i.e. an instrument that will only be used as a last option when all other mechanisms of the cybersecurity system fail or do not have a required effect.

2.6 Continuous capacity building in the field of cybersecurity

Cyberspace, as a security environment, has an unstable and constantly evolving nature, in which changes take place much more dynamically than in the physical world. Therefore, the cybersecurity governance system must adapt quickly to any changes, existing or potential threats, as well as to security challenges such as modern technologies and innovative services.

Because of a constantly changing environment, it is necessary to build continuously cybersecurity capabilities. This activity includes, in particular, the strengthening of professional personnel, development of appropriate technical tools, as well as implementation of appropriate processes for cybersecurity governance at all levels.

3. Threats

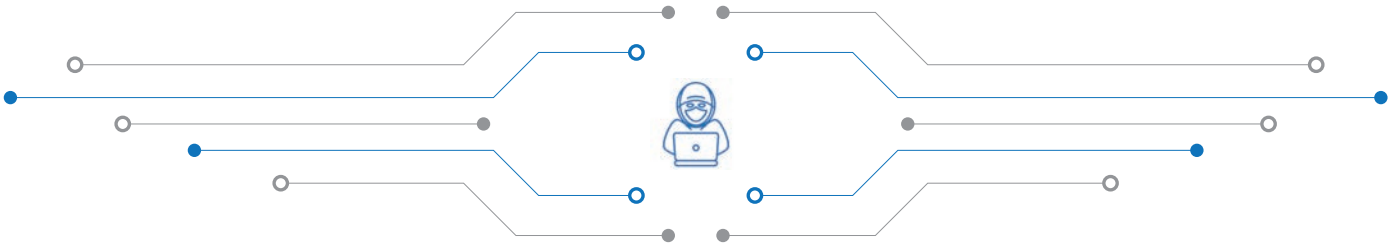
> In cyberspace, there are countless threats every day that often escalate into real attacks. Although these threats and vulnerabilities vary in nature and form and their anticipation is almost impossible, there are several specific types of threats and vulnerabilities, which if not solved, assuming in the medium-term, can cause a serious breach of cybersecurity system principles. From a strategic point of view, these are the challenges that need to be adequately addressed.

3.1 Continuous development of new techniques and methods of attacks

Just as security solutions evolve, the new techniques and methods of cyberattacks also develop. The opportunities for attackers and their tools are constantly evolving, and the response – appropriate security tools – may be late in many cases, or insufficient. Attackers respond in real time to emerging vulnerabilities in products and services, and are constantly improving in the use of social engineering methods. In addition, potential attackers have a time advantage. Preparing for an attack, preparing the tools, exploring the environment, and phishing campaigns may potentially take much longer time compared to the time available to defenders when responding to an ongoing attack. There is also a growing trend in selling of attacks and attack tools (so-called Hacking as a Service), which allows less experienced attackers to perform sophisticated and devastating attack types.

3.2 Vulnerable users

Vulnerability does not have to be only technological in nature. Just as a computer or server can be vulnerable due to security bugs in the software or due to misconfiguration, so the user himself can cause the vulnerability – for example in the form of a lack of security awareness, neglect of duties, or a low loyalty to his employer. Incorrect user interaction, insufficient risk assessment or ignorance of the basic security principles result in easy intrusion of the attacker into the organisation's systems. This can be done by one employee who for example will open a harmful attachment to an e-mail or will click on a malicious link. Rise in digitalization at the level of organisations poses a problem with an insufficiently developed culture of risk management and the dissemination of security awareness.



3.3 Attacks targeting ordinary users with (cumulative) heavy financial losses

Cyberattacks are not limited only to business entities and state institutions. Attacks on ordinary users, individuals, are also sensitive issues. Ordinary users experience the distribution of a malicious code, phishing campaigns, collection of personal data and other similar types of attacks, whereas the loss for each individual case may be relatively small, but cumulatively for each type of an attack with a wide range of victims, it can reach very high figures.

3.4 Increasing number of technological vulnerabilities

In the vast majority of cases, vulnerability is a technical gateway of the attacker to reach the victim if allowed by the victim. The number of vulnerabilities is growing in direct proportion to the development of the digital society and technological developments. The development of most new technologies is dynamic, with insufficient emphasis on security in the initial phase of their development, as the functionality and design take priority over security. There is also a problem with subsequent updates of technologies since due to a new functionality, new and serious vulnerabilities emerge or technologies lose support for updates from the manufacturer very soon after they are launched, often present with critical vulnerabilities. Technical vulnerabilities often play an important role in supply chain attacks, i.e. intentional vulnerabilities left in the product by the manufacturer or implemented by another actor in order to exploit potentially this vulnerability to their advantage.

3.5 Lack of professional staff

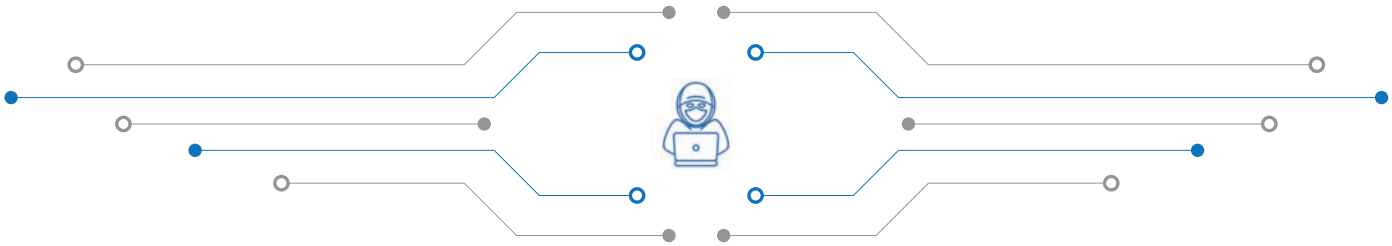
The subject of security in an organisation is not considered as a standard, but usually only as an obligation that has to be fulfilled by law. For this reason, particular entities allocate a minimum number of staff for security, who is often insufficiently qualified, lacks experience in risk management and application of security measures, and lacks sufficient support from the management and funding of their activities. Many times, the organisation's security is addressed only formally „on paper", without real implementation of basic security measures, whereas defined processes are not respected or are circumvented without taking responsibility.

3.6 Lax approach to requirements arising from legislation or standards

Implementation of security measures is a standardized operation that is determined by law, implementing regulations or a non-legislative standard. An insufficiently serious approach to such requirements leads not only to incomprehension of the existence of security measures, but also to the emergence of a weak spot of the organisation, which then becomes more vulnerable to attacks both from the outside and the inside.

3.7 Low level of security awareness

Awareness of dangers and risks in cyberspace is an area that fundamentally influences the attitude of users entering this space and their own security. The lack of users' interest in their security stems in particular from the lack of knowledge and experience in cybersecurity, making them an ideal target for attackers. In addition to this, users often lack sufficient knowledge in the field of personal data protection, which results in its leakage or provision without the necessary purpose.



3.8 Abuse of new technologies to execute attacks

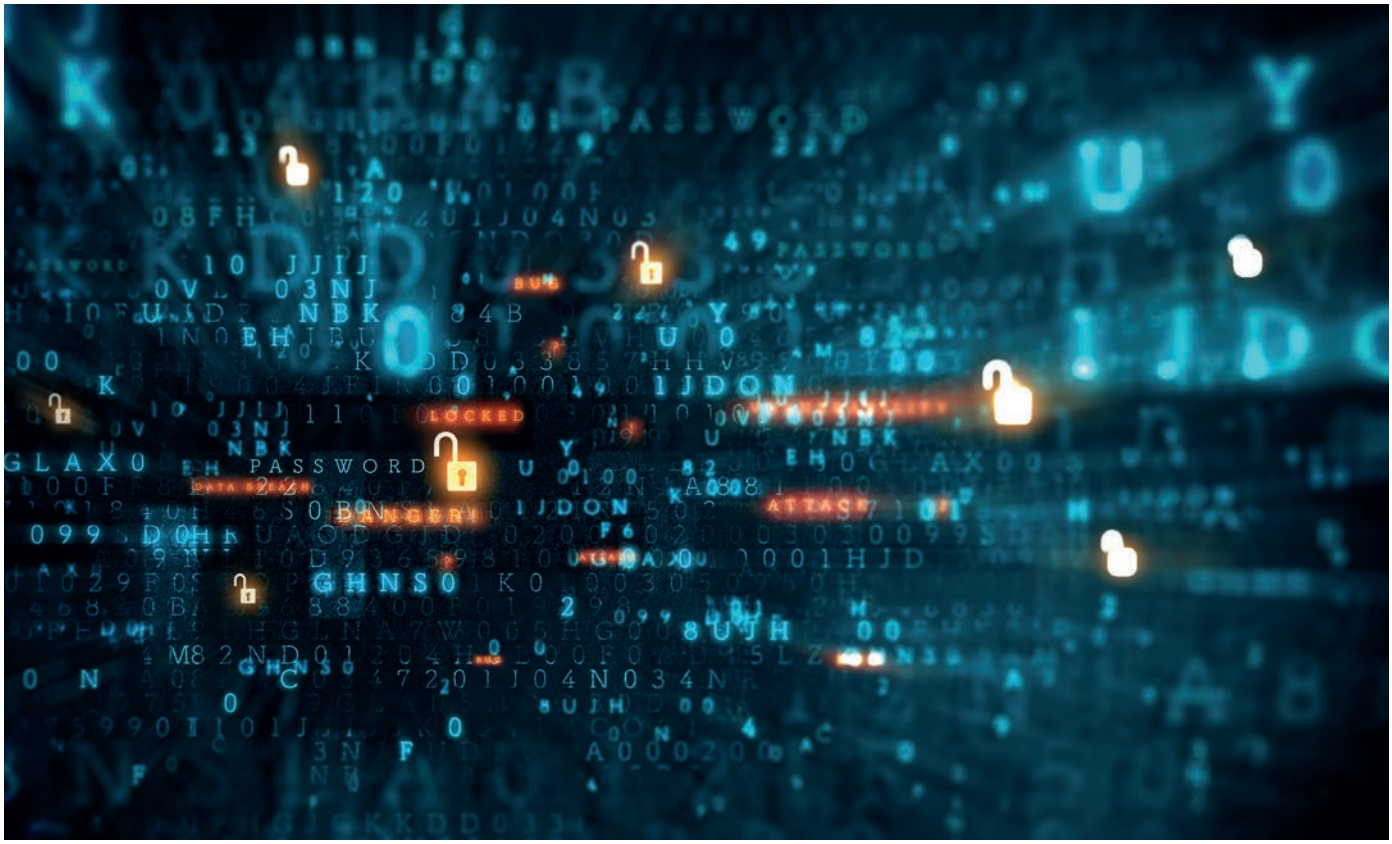
The existence and easier availability of new technologies, such as artificial intelligence applications and the Internet of Things (IoT) applications, allows attackers to execute more sophisticated cyberattacks, increases their reach and allows more efficient covering of perpetrator's tracks or complications of analytical activities in handling cybersecurity incidents.

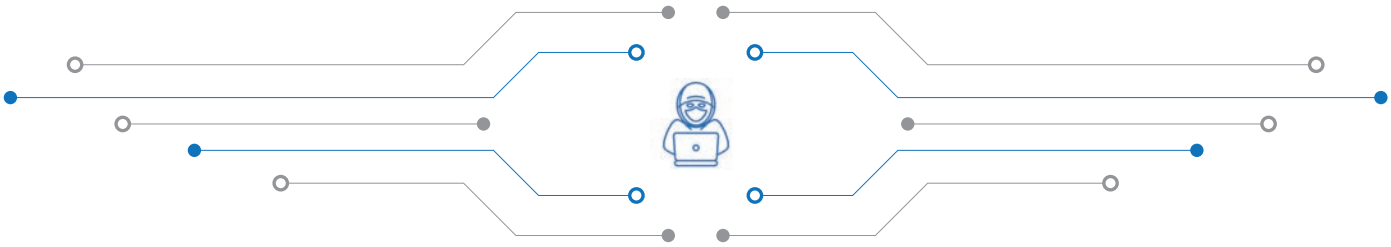
3.9 Weak detection

Detection of cybersecurity incidents, intrusion and attack attempts or successful attacks is a demanding process, requiring sufficient personnel and technical capability. At national level, several factors enter into the process, from the legislative framework that allows the state to carry out incident detection activities up to the willingness of entities to report cybersecurity incidents. If the level of detection and reporting of cybersecurity incidents does not increase continuously, it may cause incorrect conclusions leading to a reduction in cybersecurity investments, and thereby an increase in vulnerabilities of cyberspace users.

3.10 Abuse of advanced encryption techniques in cyberattacks

Attackers use data and communication encryption on several levels. First to protect the communication of their own attacking infrastructure, including the victim's devices, so that it is very difficult to decrypt such communication in real time and to detect its purpose. However, encryption is also used in more frequent ransomware attacks, in which the attacker encrypts the victim's data in order to block the access to them. This may result not only in unavailability of data but also of services provided on the devices.





3.11 Slow enforcement of criminal law in the field of cybercrime with uncertain outcomes

The term of cybercrime is not explicitly defined in the Criminal Code or in a similar normative legal act. However, the extant Criminal Code defines certain facts of crimes constituting together cybercrime. The definition stipulated in the Council of Europe Convention on Cybercrime was ratified by the Slovak Republic and will be used for the purposes of the criminal law practice.

Not every cybersecurity incident is an act of cybercrime, but every act of cybercrime is a cybersecurity incident. However, the statistical systems of prosecuting authorities do not adequately record criminal acts for facts of crimes in the field of cybercrime which reduces a real picture of the extent of this type of crime. This leads not only to the slow development of criminal law in the field of cybercrime, but also to understaffing of personnel responsible for detection and clarification of such criminal activity.

The lack of competence of investigators to investigate criminal acts in the field of cybercrime, together with the slow specialized training system for prosecuting authorities and judges, lead to an unsatisfactory speed of criminal proceedings, which often reduces the chances to detect a perpetrator of the cybercrime. This is also caused by the lack of experts and expert organisations registered in the relevant expert sectors. Another serious problem is that victims do not report a significant number of criminal acts in the field of cybercrime, and this also brings a misrepresented picture of the extent of this crime in the Slovak cyberspace.

3.12 Attacks on critical infrastructure of the state, state authorities and defence mechanisms with a power and political background

Cyberattacks are more frequently becoming a tool of jockeying for power among states. Attacks by state and non-state actors on critical assets and state institutions pose a real threat that can seriously undermine the state's security capabilities and social stability, or can cause significant economic damages.

Cyberattacks are also a tool for espionage, the purpose of which is to obtain sensitive or classified information of a foreign state and to gain economic, military or other advantage. More and more states are building offensive capabilities in cyberspace, allowing them to establish power or political dominance.

3.13 Illegal activities beyond the cyberspace

Cyberspace is also used for a spectrum of activities going beyond it. These include the dissemination of child pornography, operation of e-stores with illegal and prohibited goods, dissemination of drug addiction or extremist materials, as well as disinformation and propaganda. Although cyberspace is only a means of disseminating and sharing this content, an insufficient addressing of this issue at strategic level leads to an uncontrolled and widespread dissemination of illegal content. Cyberspace is also a domain for hybrid threats that can jeopardise the fundamental functioning of state processes, weaken citizens' trust in the state or cause a public nuisance.

4. Strategic objectives

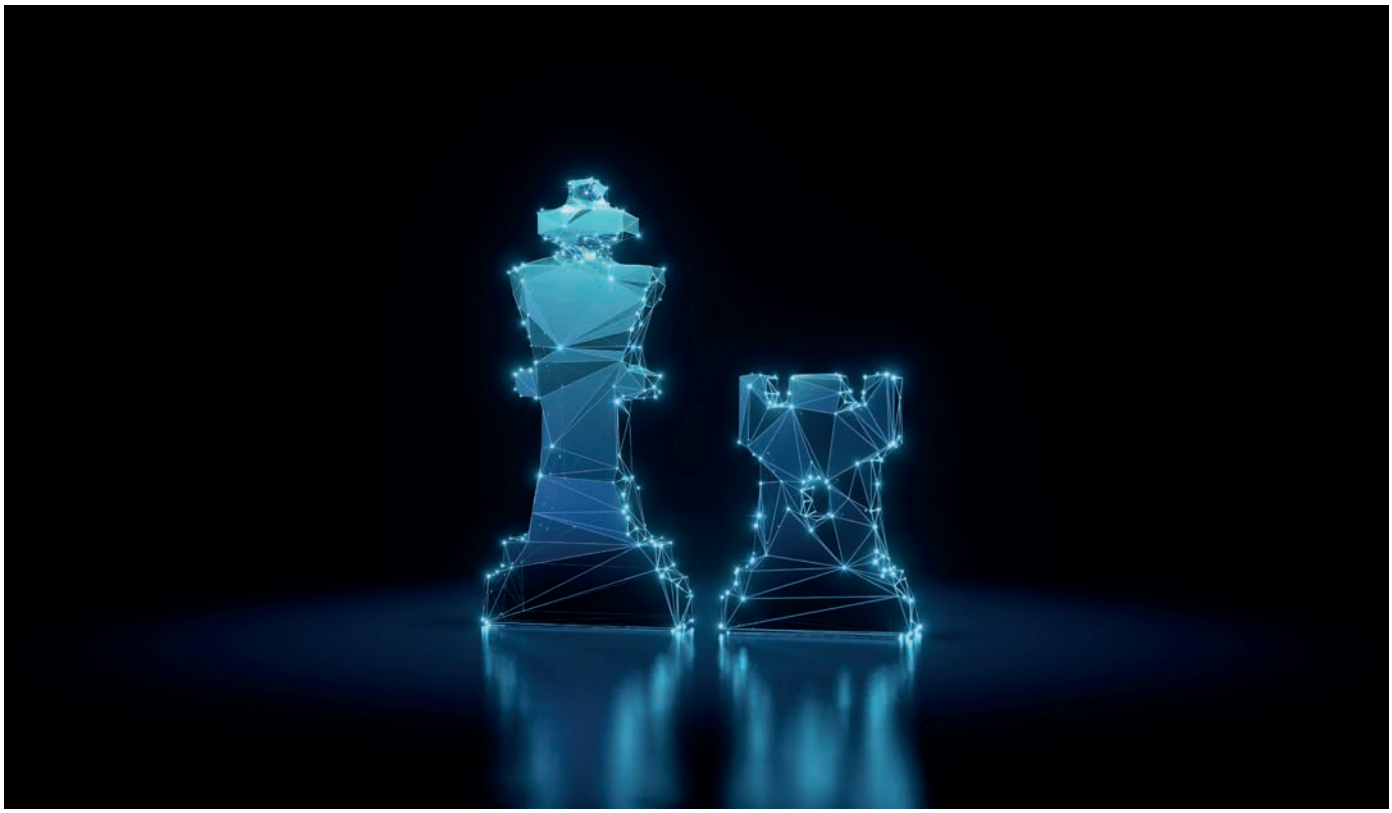
Governance of cybersecurity system does not only require well-defined rules and the implementation of necessary security measures. At national level, cybersecurity must be perceived as a strategic interest of the state, protecting state assets, and as one of the key services that the state provides to its citizens and entrepreneurs. The very implementation of the state's activities in the field of cybersecurity must be based primarily on fundamental strategic principles, while at the same time it must reflect timelessly the threats that endanger and may endanger cybersecurity and the system that governs cybersecurity at national level.

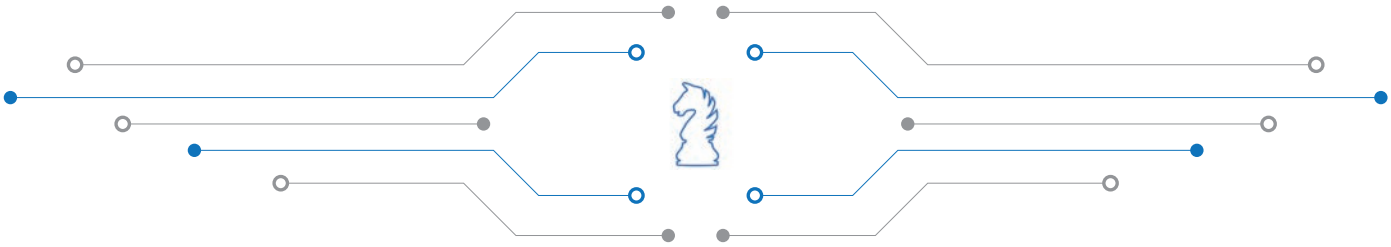
In order for the strategic principles of cybersecurity to be met and the response to threats to be sufficient, clear and measurable strategic objectives need to be set, and once they are met, it will be possible to objectively assess their impact on improvement of the cybersecurity system in the Slovak Republic.

Based on strategic principles and defined threats, the following strategic objectives have been identified.

4.1 Reliable state prepared for threats

Cybersecurity is the responsibility of every citizen of the Slovak Republic, however security cannot function without the existence of mechanisms at national level that determine the cybersecurity policy, its governance system, as well as processes for detection and handling of cybersecurity incidents, professional capacity building and dissemination of situational and security awareness. At the same time, building trustworthiness requires from the state to carry out the above activities in accordance with the Constitution of the Slovak Republic and other laws and apply fundamental human rights and freedoms only to a necessary extent.





4.1.1 Initial conditions

The state is gradually building cybersecurity capacities and capabilities, addressing in particular the shortage of professional personnel.

The state relies on the citizen being the end user of any security services, but without providing him with sufficient information on how to use these services safely.

The state is gradually developing competencies and capabilities in the field of certification of cybersecurity products, processes and services.

The state is gradually building capabilities to detect and handle cybersecurity incidents, focusing on capability development mainly at national, not sectorial level.

There is no uniform process for attributing cybersecurity incidents and subsequent diplomatic and legal mechanisms.

Detection of incidents in respective sectors and in critical infrastructure and their subsequent reporting to authorities have major shortcomings, thus reducing the visibility and knowledge of the cybersecurity authority about the status of cybersecurity.

The state is gradually building competence for conformity assessment and cybersecurity audit.

Cybersecurity risk management across sectors is carried out unsystematically or is not carried out at all.

4.1.2 Goals to be achieved

Building a sufficient professional personnel base for the information and cybersecurity governance system not only at national level but also at sectoral level.

Cooperation between the state and the citizen at the level of providing sufficient information and recommendations, and the implementation of actions that the citizen will tangibly experience as an increase in their own security and the security of the national cyberspace.

Creation and use of certification schemes for a wide portfolio of product types, processes and services.

More improved technical, organisational and personnel security, based on the use of modern approaches to cybersecurity for detection and handling of cybersecurity incidents.

Capability development to detect and handle cybersecurity incidents at all levels.

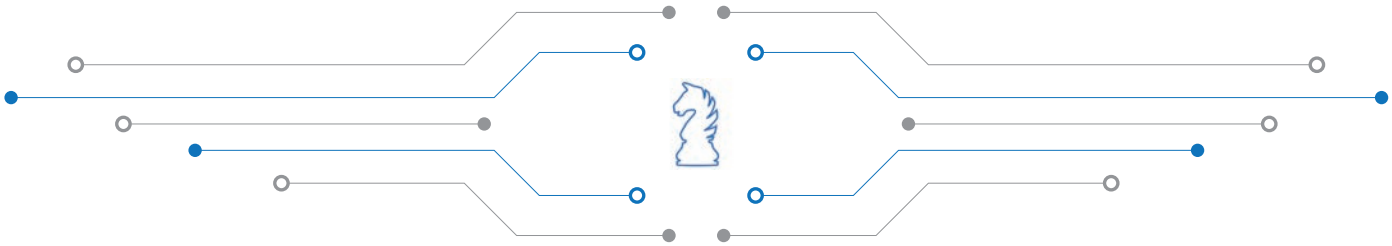
Effective cooperation of stakeholders at all levels in addressing information security and cybersecurity.

A well-configured process of technical, as well as political attribution of cybersecurity incidents.

Systematic and continuous cybersecurity risk management across sectors.

Improving the detection of cybersecurity incidents at sectoral level, improving and simplifying the cybersecurity incident reporting not only for liable entities, but also in voluntary reporting.

Support of the competence of entities in the field of business continuity management.



4.1.3 How to achieve the goals

In order to achieve the goals of this strategic objective, it is necessary to focus on:

- creation of the concept of „safe Internet for all", which combines the enormous efforts of the state to ensure a high level of cybersecurity with the responsibility of individuals for carrying out activities aimed at their own security,
- flexible response of the state to new technologies, so that a risk analysis is always carried out and the possible security impacts of these technologies on the essential and critical assets of the state as well as on the citizen, are defined,
- preparation of legislative proposals, which will be comprehensible, actually applicable and will not impose disproportionate economic, personnel or organisational costs on liable entities,
- integrating of extant regulations in the field of cybersecurity so that respective entities do not have to apply multiple legal regulations on the same issue,
- holding a professional dialogue of the state with stakeholders and professional associations in case of amendment of legislation and rules of regulation,
- introducing viable cybersecurity risk management processes,
- development of certification as a tool for more trusted products, processes and services in the field of cybersecurity,
- implementation of European certification schemes in the field of cybersecurity into national certification procedures,
- application of a coherent concept of crisis management in the field of cybersecurity, with links to integrated national and international mechanisms,
- continuous strengthening of technical, organisational and personnel capacities for detection and handling of cybersecurity incidents at national level and within individual sectors, including the critical infrastructure,
- effectiveness and legitimacy of services provided for the citizen in the field of cybersecurity,
- establishment of a viable system of continuous capacity building of professional personnel,
- development of capabilities in the field of detection and collection of security-relevant events in the national cyberspace, as well as development of capabilities in the field of event evaluation and incident detection by modern techniques in the national cyberspace using various forms, algorithms and technologies, including the artificial intelligence,
- development of capabilities in the field of security incident handling and automation of processes in this area using machine learning, as well as development of capabilities to respond to severe security incidents on site at operators of essential services with the necessary equipment and capacities,
- integrating of extant escalation procedures for incident reporting so that respective entities do not have to apply multiple legal regulations on the same issue,
- creation of a technical and political incident attribution process, together with determination of responsible institutions and legal mechanisms and mechanisms of cyber diplomacy,
- strengthening of analytical capacities in the field of security threats, specializing in cybersecurity incident attribution,
- effective performance of active and passive cyber intelligence aimed at gathering, aggregating and evaluating of information on activities in cyberspace, posing a threat to the security of the Slovak Republic,
- setting up rules and mechanisms for blocking of abusive content, especially control servers of attackers, devices spreading malicious code and devices attacking foreign infrastructure for the purpose of denial of service,
- development of education and training concept for personnel in public administration, aimed at recruitment, maintenance, security and career progression, as well as increasing and maintaining their professional competence,
- creation of suitable motivational and reward tools for professional staff in public administration in order to balance conditions of public administration and the private sector.

4.2 Effective detection and clarification of cybercrime

The number of cybersecurity incidents, which are also criminal acts of cybercrime, is constantly increasing. Attackers are more sophisticated, and attacks are more difficult to detect. Victims suffer great damage, which poses a threat to their economic existence. Cyberattacks are very well organised and well timed and attackers usually sweep their tracks very well, and their detection is very difficult. The attribution of attackers is a very demanding process that requires sufficient personnel and well-configured processes.

4.2.1 Initial conditions

Cybercrime, or criminal acts of cybercrime are settled in legislation but practical enforcement of the law in this area faces legislative obstacles that complicate operative detection and clarification of this type of crime.

Criminal acts of cybercrime are often not reported, and therefore the real extent of this type of crime at national level is not visible.

Legislation at international level is not unified.

Prosecuting authorities do not have sufficient capacities to fight cybercrime, particularly at the level of basic departments when reporting this type of criminal act.

The National Expert Group on Fight against Cybercrime operates at national level, associating both state organisations and some private sector organisations.

There is a national network of prosecutors to fight cybercrime. The Public Prosecutor's Office of the Slovak Republic is also involved in the European Judicial Network to fight cybercrime and cooperates with Eurojust and other national and international organisations.

Education in the field of cybercrime takes place through specific activities of the Public Prosecutor's Office, the Police Force and the Judicial Academy of the Slovak Republic.

4.2.2 Goals to be achieved

> Sufficient capacities allocated to fight cybercrime, effective cooperation of stakeholders, speed of criminal proceedings, as necessary for detection and clarification of cybercrime.

More criminal acts of cybercrime reported and investigated.

Better coordination of procedures in the field of cybercrime and their integration at international level.

Active cooperation in the field of cybercrime between stakeholders at national level and sharing of relevant information.

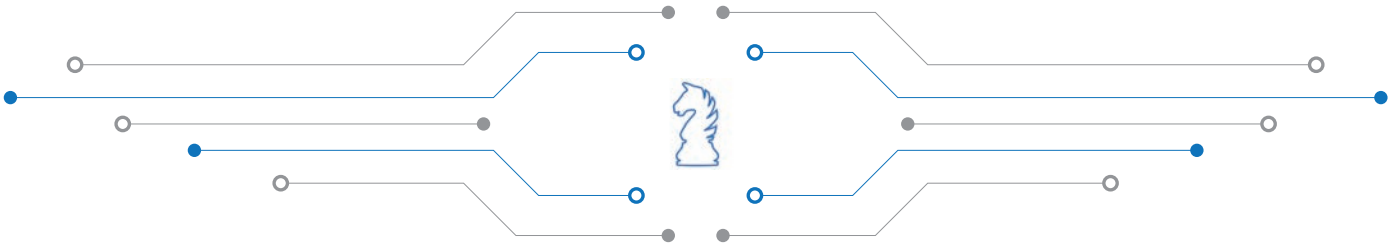
Specialization of prosecuting authorities in the field of cybercrime from basic departments of the police force up to the public prosecutor's office and courts.

Development of education activities in the field of cybercrime.

4.2.3 How to achieve the goals

In order to achieve the goals of this strategic objective, it is necessary to focus on:

- streamlining and acceleration of operational and investigative procedures in the field of detection and clarification of cybercrime,
- allocation of sufficient personnel capacities to solve cybercrime at the level of regions and districts so that there is a sufficient number of specialists among operative staff, investigators, prosecutors and judges specialized in this area,
- improving cooperation between entities involved in cybercrime,
- accelerating the response of the legal system to emerging threats in the field of cybercrime,
- defining the term of cybercrime in the Criminal Code,
- continuing a dialogue on integration of cybercrime processes at international level,
- improving the education framework for prosecuting authorities and courts in the field of cybercrime,
- continuous raising of security awareness in the field of cybercrime with a focus on wide range of population and the most vulnerable groups (children and seniors).



4.3 Resilient private sector

Operators of essential services in the private sector are a key element in providing a wide portfolio of services to citizens, the private sector as well as the public administration. According to the Act on Cybersecurity and the Act on Critical Infrastructure, elements of critical infrastructure are stipulated by default as essential services and their operators are operators of essential services. These services and their operators are extremely critical to ensure a smooth running of companies. These companies have a large number of customers or a significant economic impact, an important role in the protection of human life and health, the impact on public order and security, and the impact on the mobility of persons or the transport of goods. Their security is therefore an important factor, enabling not only the continuous provision of essential services, but also their development.

4.3.1 Initial conditions

There are major differences in cybersecurity and in the implementation of security measures of operators of essential services across different sectors. Operators of essential services, even in the private sector, take cyber regulation only as another legal obligation. Operators of essential services take application of corresponding security measures vaguely, to a large extent, which stems mainly from their weak security awareness in the field of cybersecurity and information security.

The Act on Cybersecurity has a cross-sectional nature, and therefore introduces only minimum security requirements that can be implemented uniformly across all sectors. However, these uniform minimum requirements are not sufficient in several sectors.

4.3.2 Goals to be achieved

> Sector-specific security requirements complementing the basic minimum legal requirements, ensuring high-level cybersecurity, with regard to sectoral needs and specifics.
>
> Cybersecurity awareness of operators of essential services and operators of critical infrastructure in the private sector as an essential part of their operation, not just as further state regulation.
>
> Well-functioning public-private cooperation not only in the field of regulation, but especially in sharing of security information, experience and in further development.

4.3.3 How to achieve the goals

In order to achieve the goals of this strategic objective, it is necessary to focus on:

- a sector-specific approach in the field of cybersecurity, focusing on sector specifics,
- providing support to both operators of essential services and operators of critical infrastructure in the private sector in taking of appropriate security measures,
- development of effective cooperation, information sharing and expert discussion of the public sector and the private sector.

4.4 Cybersecurity as an essential part of public administration

Not only the services provided by private companies but also those provided by the state must function well in cyberspace. The services provided by the state to its citizens must be secured adequately to prevent abuse of sensitive or personal data in the context of Regulation (EU) 2016/679 of the European Parliament and of the Council. Operators of essential services operating within the public administration are a specific category and their security must be an essential part of their existence.

4.4.1 Initial conditions

Operators of essential services in the public sector often respond vaguely to the obligation of taking appropriate security measures, mainly due to a lack of security awareness among operators and their suppliers in the field of cybersecurity and information security. Cybersecurity in public administration has additional security regulation as stipulated by the Act on Information Technology in Public Administration; however, this regulation is often not implemented or sufficiently implemented. Designing the state's IT infrastructure has usually not respected or does not respect security rules and the situation is the same for its operation.

The security of the state's electronic services has not been evaluated in the long term and the security aspect is not provided sufficiently to the citizen.

4.4.2 Goals to be achieved

> The „security by design" rule as mandatory in the design, procurement, creation, implementation and operation of the state's systems and services.

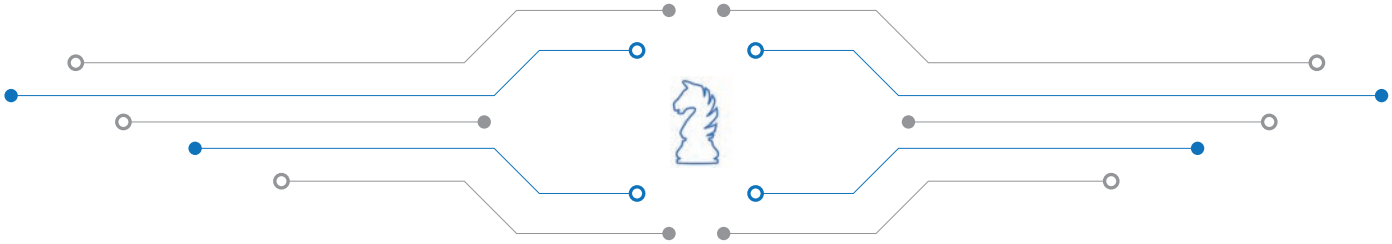
A citizen must perceive that the services provided by the state, as well as their own activities, are safe.

Risk management of cybersecurity and information security in public administration must be a viable process that minimizes risks at all stages of the system's life cycle from preparation of specification, procurement, architecture design, implementation, operation and maintenance up to decommissioning. The governance of cybersecurity and information security must be a natural part of the governance of public administration information systems.

4.4.3 How to achieve the goals

In order to achieve the goals of this strategic objective, it is necessary to focus on:

- application of a systematic approach to cybersecurity based on risk analysis and risk management in each relevant area, whereas each analysis must be based on the plan and methodology of integrated risk analysis and risk management,
- providing the state's secure and accessible electronic services to each citizen, with the possibility of an adequate equal use of electronic tools,
- improvement of the process of design, procurement, creation, implementation and operation of the state's IT infrastructure, from the beginning paying attention to cybersecurity so that vulnerabilities or threats do not arise when using these services (paying attention to the principle of "security by design"),
- improvement of professional capacities in public administration,
- increase in protection of operators of essential services in public administration from the perspective of cybersecurity so that their audit and regular inspections of implemented measures will permanently demonstrate a positive trend in improving the situation of cybersecurity in public administration,
- setting up security rules of a supply chain for the state's IT infrastructure so that unforeseen security incidents can be prevented and the supplier cannot obtain a specific or exclusive position, which could jeopardise the security of the operation of the state's IT infrastructure,
- giving continuous and comprehensive support of cybersecurity solutions and governance to organisations of public administration from the central level.



4.5 Strong partnerships

Security in general is one of the primary interests of any democratic country with the rule of law. The field of cybersecurity is no exception, and it is more globalized as cyberattacks do not recognize national borders and attackers need not be explicitly citizens of the country in which the attack originates from. Therefore, it is very important that the state creates very strong partnerships at international level, exchanges experiences, knowledge and information, and afterwards applies them at national level. Cooperation and confidence building between entities of public administration, the private sector and academia ensures the cybersecurity development.

4.5.1 Initial conditions

The state is gradually building and maintaining cybersecurity relations, in particular at the level of the European Union (EU), the United Nations (UN), the North Atlantic Treaty Organization (NATO), the Council of Europe and the Organisation for Security and Co-operation in Europe (OSCE). It also has concluded bilateral agreements (memorandum of understanding) with several countries and supports selected international initiatives in order to strengthen international cybersecurity.

The Slovak Republic actively participates in the processes of policy-making and strategic documents creation in the international environment. It is also involved in common mechanisms for confidence building and capacity building.

The National Cyber Security Centre SK-CERT is an active member of the European network of national CSIRT units. Various Slovak CSIRT units are active members of international CSIRT organisations.

At national level, the state builds relations with operators of essential services and digital service providers, through both formal and informal channels.

The state is also active through its representatives in the European Union Agency for Cybersecurity (ENISA), and develops its activities in the network of national cybersecurity competence centres.

The Slovak Republic actively cooperates with the NATO Cooperative Cyber Defence Centre of Excellence.

4.5.2 Goals to be achieved

> The Slovak Republic as a respected state with good representation abroad through professionally competent representatives at both technical and political levels.

A healthy and strong partnership network established at national level between the state authorities, the state and the private sector, as well as academia and the professional public.

A network of cybersecurity competence centres established at the European level, including the Slovak Competence and Certification Cyber Security Centre as a national representative in the Governing Board of the European Competence Centres.

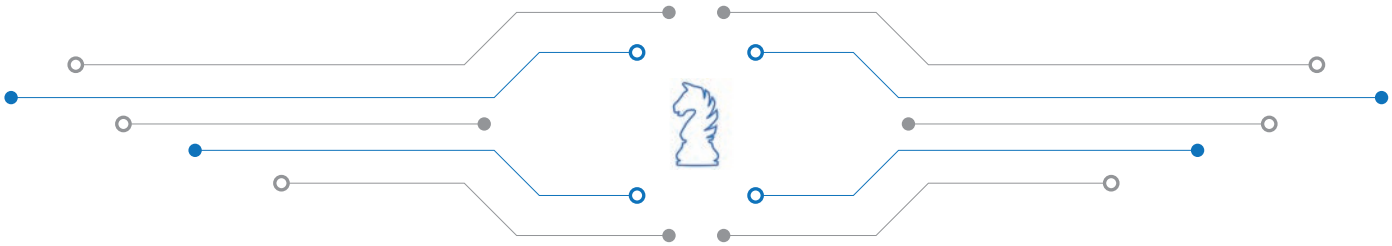
Increased involvement of the Slovak Republic in the activities of the European Cyber Security Organisation (ECSO).

Defining the main foreign policy partners in the field of cybersecurity.

4.5.3 How to achieve the goals

In order to achieve the goals of this strategic objective, it is necessary to focus on:

- strengthening existing international partnerships and creating new ones, especially with countries whose political and security system is based on freedom and democracy,
- development of political cooperation in the field of cybersecurity,
- development of cyber diplomacy through position establishment of thecyber-attaché, as well as by using current capacities of representative offices of the Slovak Republic abroad,
- building strong partnerships at national level between the various state authorities involved,
- active involvement in the international environment aimed at enforcing of norms of responsible behaviour in cyberspace,
- development of the state cooperation with operators of essential services and digital service providers,
- increasing awareness and communication with the public in the area of cybersecurity priorities,
- deepening the partnership of the state with academia,
- strengthening the exchange of information and experience with partners, creation of organisational and technical platforms,
- establishment and maintenance of the national CSIRT network, which will unite Slovak CSIRT units (state-run as well as private ones),
- involvement of the Competence and Certification Cyber Security Centre in the Governing Board of the European Competence Centres as a national representative,
- establishment and coordination of sectoral ISACs,
- close cooperation with the Cyber Defence Center of the Slovak Republic, the authority for cyber defence of the state,
- deepening cooperation of states in the field of cybersecurity with a focus on creating binding security standards for manufacturers of information technologies,
- building cooperation of the state with the private sector, especially with companies specialized in cybersecurity solutions and innovative technologies.



4.6 Well-educated professionals and well-educated public

In the field of cybersecurity, education is one of the main areas allowing development and improvement of capabilities in comprehensive activities of the cybersecurity system. Building situational and security awareness, towards ordinary users, acts as a precaution against cybersecurity incidents, because educated users can better respond to security threats and risks in cyberspace and behave responsibly enough to prevent successful attacks, which can occur due to their low awareness. It is important to understand security awareness raising as an entire educational process, when a person being educated not only understands the issue, but is also able to identify it.

4.6.1 Initial conditions

Cybersecurity education is not systematically addressed, there are very few cybersecurity university programmes. It is also related to a lack of teachers in the cybersecurity field. There are several specialized courses and trainings in the commercial market, but they cannot replace systematic education.

Security awareness building and basic security education in the area of responsible behaviour on the Internet from primary schools up to secondary schools is missing, despite the fact that a significant number of users is already emerging at these levels.

The education of public administration staff is not systematic, there is no basic security education system for public administration officials who work daily with information systems of public administration and are exposed to sensitive and personal data.

The private and third sectors are working in a decentralized form to educate and raise security awareness in the field of cybersecurity at different levels of education and in different sectors.

Situational and security awareness is built unsystematically, often only in the form of a response to current problems, with little impact.

4.6.2 Goals to be achieved

- A sustainable vocational higher education system and specialized trainings as forms of further education in the field of cybersecurity and information security.

- The concept of basic security education at all levels of education, from primary schools to universities.

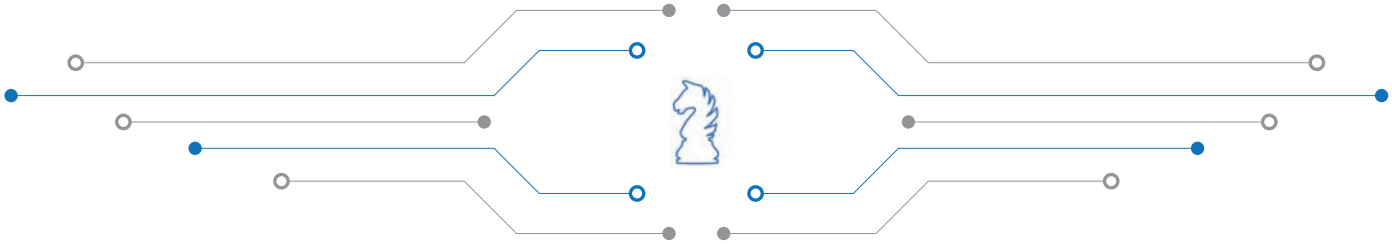
- Systematic, broad-spectrum and planned situational and security awareness raising based on a reliable system that responds flexibly to changes in cyberspace.

- Educated public administration staff who can safely provide services and use public administration systems without emerging cybersecurity incidents due to their low security awareness.

4.6.3 How to achieve the goals

In order to achieve the goals of this strategic objective, it is necessary to focus on:

- establishment of a vocational higher and secondary education system, which will ensure the education of new professionals,
- establishment of a system of specialized trainings for professionals in the field of cybersecurity and information security,
- establishment of a system for raising a security and situational awareness of threats, vulnerabilities, incidents and protection procedures in cyberspace,
- establishment of a system of education for public administration staff so that they meet minimum knowledge standards in the field of cybersecurity and information security,
- completing and maintaining the competencies in cybersecurity and information security through the Slovak Qualifications Framework and the National Qualifications System of the Slovak Republic,
- developing the concept of minimum security awareness requirements for all levels of education,
- integration of roles in the field of cybersecurity and information security into the National Qualifications Framework,
- implementation of joint educational activities and activities supporting security awareness raising with public authorities, academia and the private sector,
- development of capabilities in the field of exercises and trainings in technical and process areas by means of various forms, together with the creation of an appropriate technical and organisational platform for organizing such exercises,
- support of projects and programmes in the field of education and security and situational awareness raising.



4.7 Building research and development capabilities in the field of cybersecurity

Threats and vulnerabilities in cyberspace are constantly evolving with the technological development and digitalization of society. Research and development in the field of cybersecurity is an appropriate mechanism for responding to a change in the security environment and implementing appropriate measures in order to minimize threats, mitigate vulnerabilities, detect and handle cybersecurity incidents.

4.7.1 Initial conditions

Research and development in the field of cybersecurity is decentralized and minimal, mainly addressed by private companies within their business activities and academia.

The state does not have a comprehensive concept of the state support for research and development in the field of cybersecurity; it does not have uniform objectives defined in this area.

4.7.2 Goals to be achieved

"Well-functioning and state-supported research and development in the field of cybersecurity.

A good communication between the public sector, the private sector and academia in the field of research and development with clear outcomes.

An effective system of cooperation between the public sector, the private sector and academia.

State support of cybersecurity projects and active state assistance in the use of European funds.

4.7.3 How to achieve the goals

In order to achieve the goals of this strategic objective, it is necessary to focus on:

- creation of a comprehensive concept of the state support of research and development in the field of cybersecurity for the Slovak Academy of Sciences, universities and commercial organisations,
- allocation of financial resources for the state support of research and development for the next 5 years,
- support of research centres in the field of cybersecurity at universities,
- development of capabilities in the field of national cryptography,
- support of scientific and research projects of private companies and research centres at national level,
- assistance and support to entities in their participation in scientific and research programmes and grants at national and international level,
- participation in the promotion of national research programmes and their results,
- establishment of a closed research network infrastructure across the whole Slovak Republic oriented on cybersecurity research, development and testing,
- coordinating the support of science and research through the Competence and Certification Cyber Security Centre.

5. Main foreign political partners

> As cyberspace goes beyond the national borders, the international cooperation is crucial for achieving desired objectives of cybersecurity.

The Slovak Republic is a democratic country with the rule of law based on the principles of respect for fundamental rights and freedoms. Therefore, within the international cooperation in the field of cybersecurity, it focuses on political and technical cooperation with the states and international organizations that respect and promote the same values.

The Slovak Republic, as a member of the EU, fully supports the common foreign and security policy, respects and cooperates with individual Member States, and develops common cybersecurity capabilities at the all-European level. It includes mainly its membership in the European network of CSIRT units at the technical level, at the political-strategic level it is a membership in the Horizontal Working Party on Cyber Issues, or in working groups of the European Commission.

The Slovak Republic's membership of NATO is a good model in terms of security, ensuring the collective defence of its members and partners, and maintaining peace not only in Europe for several decades. NATO focuses mainly on cyber defence issues, because an increasing number of cyberattacks and also hybrid threats have posed new challenges for the Alliance that need to be addressed through deterrent defence capabilities, as well as through continuous capability development not only at the level of Member States and partner states, but also through joint activities, such as the NATO Cooperative Cyber Defence Centre of Excellence.

The Slovak Republic's membership of the UN and the OSCE enables its active participation in activities and projects in the field of cybersecurity, organized and created by mentioned organizations.

Positions of the Slovak Republic in international fora dealing with cybersecurity issues are based on the principles of global, open, free, stable and secure cyberspace, while fully respecting the fundamental principles of the rule of law, human rights and fundamental freedoms, gender and digital equality as well as sustainable development. The Slovak Republic, together with partners within the EU, emphasizes the importance of international standards and rules for responsible behaviour in cyberspace, the development and implementation of confidence-building measures and capacity building in the field of cybersecurity. The Slovak Republic will use the tools of cyber diplomacy towards perpetrators of cyberattacks targeting the Slovak Republic and its interests, and in compliance with its commitments to the EU, NATO and its allies.

6. Implementation and measurability

> In order to successfully achieve the strategic objectives of the National Strategy, its corresponding Action Plan must be created, as well as a Steering Committee at the level of which the actions of stakeholders will be coordinated.

6.1 Creation of the Action Plan

The Action Plan for the implementation of the National Cybersecurity Strategy 2021-2025 will determine:

- specific tasks and activities divided according to strategic objectives,
- method of implementation of individual tasks and activities,
- responsible entities in the role of entities in charge and stakeholders,
- time period for the performance of tasks,
- impacts or costs incurred by individual tasks.

The National Security Authority will be responsible for drawing up the Action Plan, and will involve all stakeholders in its preparation.

6.2 Establishment of a Steering Committee for the implementation of the National Strategy and the Action Plan

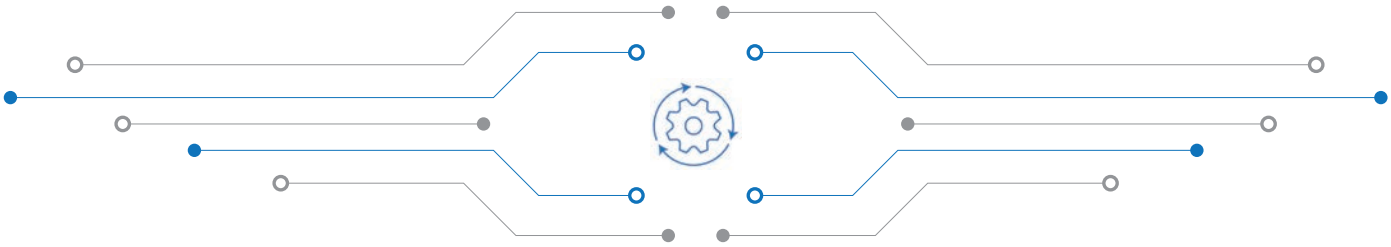
For better management of respective tasks and activities, a Steering Committee will be established, which will be the coordination body for all stakeholders who can appoint their representatives therein. The platform of this working group will communicate the process of implementation of individual tasks and activities and will also address the problems arising during the implementation of the Action Plan. The Steering Committee will also prepare a regular report on the fulfilment of the Action Plan. The National Security Authority will be responsible for the organisation and management of the Steering Committee.

6.3 Implementation

The National Strategy will be implemented through the Action Plan and its tasks and activities. The implementation of respective tasks and activities will be the responsibility of the entities appointed in the Action Plan, either as entities in charge or stakeholders.

6.4 Measurement

Appointed entities will be responsible for the fulfilment of respective tasks and activities, and the National Security Authority will be responsible for the evaluation of the implementation of the Action Plan. The review and evaluation of the implementation of the Action Plan will be carried out once a year.



6.5 Stakeholders

Key stakeholders in the cybersecurity system of the Slovak Republic include, in particular:

- Government Office of the Slovak Republic,
- National Security Authority,
- Ministry of Investments, Regional Development and Informatization of the Slovak Republic,
- Ministry of Finance of the Slovak Republic,
- Ministry of Foreign and European Affairs of the Slovak Republic,
- Ministry of Defence of the Slovak Republic,
- Ministry of Education, Science, Research and Sport of the Slovak Republic,
- Ministry of Interior of the Slovak Republic,
- Ministry of Justice of the Slovak Republic,
- Ministry of Health of the Slovak Republic,
- General Prosecutor's Office of the Slovak Republic,
- Office for Personal Data Protection of the Slovak Republic,
- Presidium of the Police Force of the Slovak Republic,
- Military Intelligence,
- Slovak Information Service,
- universities and other educational institutions,
- Cybersecurity Competence and Certification Centre,
- operators of essential services,
- digital service providers.

7. Financing

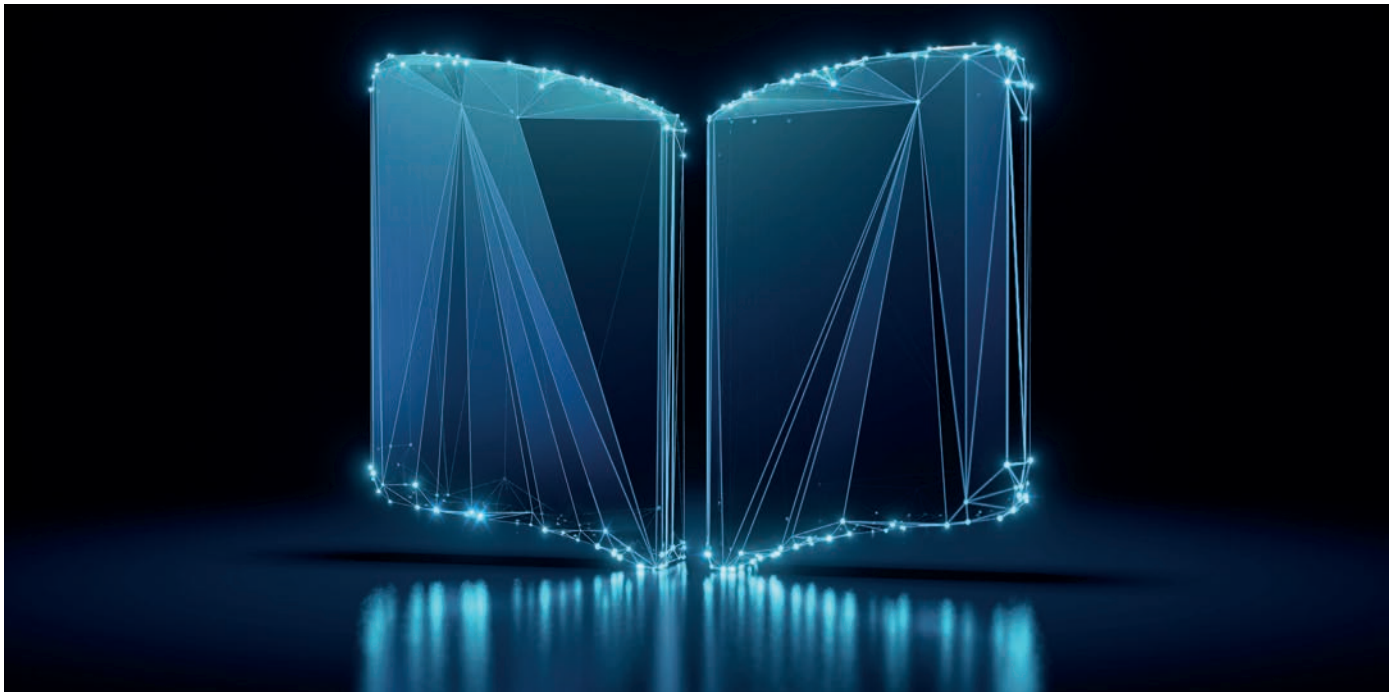
Each of the responsible entities within the cybersecurity system, also defined in the follow-up Action Plan, must allocate sufficient funds within their budget sections to fulfil the tasks and activities based on their approved Action Plan, as well as on the principles of the cybersecurity system. In the search for financial resources, it is necessary to rely not only on resources from the state budget but also on resources from the operational programmes of the European Community funds.

It must be in the interest of the state and its organisations and institutions to allocate sufficient funds for cybersecurity at all levels so that the strategic cybersecurity objectives as defined in the National Strategy can be met.

8. Conclusion

Cyber threats are no longer just a matter of special systems and IT professionals. They concern each of us. Cybersecurity must be a shared responsibility of the state and its citizens. Attacks by foreign powers as well as activities of cybercriminals have a significant impact on our daily lives. The primary strategic interests of the Slovak Republic must include maintaining and improving the cybersecurity system so that threats, vulnerabilities and incidents have the least possible impact on the state and its citizens, as well as on the functioning of the social system.

The National Cybersecurity Strategy for the years 2021-2025 is a medium-term document. It will be adopted for a period of 5 years. In the event of a change in the security environment or in the event of other impacts that could significantly affect the functioning of the cybersecurity system in the Slovak Republic, the document may be updated earlier.



NATIONAL SECURITY AUTHORITY

NATIONAL CYBER SECURITY CENTRE SK-CERT

Budatínska 30, 851 06 Bratislava

www.nbu.gov.sk

www.sk-cert.sk