Cyber Security Concept of the Slovak Republic

for 2015 - 2020

ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

NASES
NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY

NBÚ

Cyber Security Concept of the Slovak Republic

for 2015 - 2020

Content

Foreword

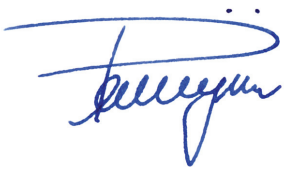
The dependency of today's society on information and communication technologies increases every day; over the past decade, these have changed and impacted almost every aspect of our lives. Human activities are slowly but surely shifting, to a large extent, from physical space to cyberspace. On the one hand, information and communication technologies make our lives easier, speeding up communication and access to information and services. On the other hand, however, the increasing dependency of the public and private sectors on these technologies, if insufficiently protected, renders them more vulnerable, making cyber security one of the most important challenges the state has to face today. Globalism and the significance of impacts of potential cyber attacks have resulted in the need for a conceptual and coordinated control of protection and defence of cyber space.

By adopting this Concept, the Slovak Republic has established its visions and priorities providing for cyber security in the country. The Concept has to be seen as the "cornerstone", the basic and starting document for the subsequent formulation of legislation, standards, methodology, rules, security policies and other tools necessary for ensuring the protection and defence of national cyber space.

The Concept, based on a strategic and methodological framework shaped in NATO, EU, OECD and UN documents for the area of cyber security, proposes the adoption and priority treatment of seven key measures; the implementation thereof will be specified in a material, time and financial plan in the form of a Concept Implementation Action Plan. The purpose of cyber security in the Slovak Republic, as seen by the Concept, should be an open, secure and protected national cyber space, i.e. the building of trust in the reliability and security of, without limitation, critical information and communication infrastructure, as well as the building of certainty that this infrastructure will fulfil its functions and also serve national interests in cases of cyber attacks.

Cyber security ought to be perceived as one of the key components of national security. It is a complex field involving both legal and technical aspects and required trust and collaboration of the public sector, private sector and academic institutions. The rights, duties and tasks of individual actors in cyber space will be soon established by adopting and creating an institutional and legal framework of cyber security; the Cyber Security Act will certainly form a substantial milestone in the perception of cyber security in the Slovak Republic.

Cyber security can only be achieved using mutual trust and collaboration since it is only by making mutual efforts that we can succeed in building both an open and secure cyber space from which we all may benefit.



Peter Pellegrini
Speaker of the National Council
of the Slovak Republic
Digital Champion
of the Slovak Republic

Róbert Fico
Prime Minister
of the Slovak Republic

1 Introduction

The exponential growth in the use of information and communication technologies from the second half of the 20th century onwards has significantly influenced development trends in society. Modern information and communication technologies have substantially broadened the possibilities and increased the efficiency of the interaction methods between geographically remote entities from various fields of the society and economy. The growing number of users of information and communication technologies results in an increasing dependency of both the public and the private sectors on these technologies, rendering them more vulnerable.

Besides the high dependency of society on information and communication technologies, the beginning of the 21st century was marked by a significant change in the global security environment and an increasing number of asymmetrical threats with a higher degree of sophistication and impact effects. A wide scope of potential methods of abuse and damage to electronic information, communication and control systems as well as of a negative influencing of social and economic processes in the framework of the international cyber environment thus included cyber threats among potentially serious global threats such as international terrorism, proliferation of weapons of mass destruction, etc.

Critical control, technological, communication and security systems are endangered by new forms of attacks, and so are those services that would, if failing or malfunctioning, seriously impact the operation of the state (mostly in its main security areas). Dynamically developing modern technologies make it possible for additional new security threats to emerge.

The Slovak Republic must be prepared to react to a wide spectre of existing and potential threats. At the same time, it is aware of the fact that threats and attacks emerging in cyber space may escalate up to a level that would require collaboration of the allies within the North Atlantic Treaty Organization (hereinafter referred to as "NATO") under Article 5 of the North Atlantic Treaty[1] that would result in a collective defence and/or coordinated response. Thus, cyber security also needs to be perceived as a subsystem of national security and cyber space as its new operational domain. The Slovak Republic intends to cooperate with all relevant state and private cyber space actors, which respect identical values and do not restrict the freedom and safety of the use of cyber space.

This Cyber Security Concept of the Slovak Republic for the years 2015-2020 (hereinafter referred to as the "Concept") defines the starting position and the goals of the Slovak Republic in the field of cyber security. The Concept is harmonized with the Security Strategy of the Slovak Republic and forms a basic and starting document for the subsequent creation of regulations, standards, methodical instructions, rules, security policies and other instruments necessary to provide for cyber security.

1 *The North Atlantic Treaty dated 4 April 1949, the so-called Washington Treaty, establishing the North Atlantic Treaty Organization (NATO).*

2 Basis and Principles of Cyber Security

The Concept is based on a statement and a description of the basic terms and principles, characteristics of the current situation of the strategic, legal and institutional frameworks in the area of cyber security in the Slovak Republic and on a strategic and methodological framework formed by NATO and European Union (hereinafter referred to as the "EU") documents; subsequently, the Concept formulates principles, goals and proposed solutions.

2.1 Basic Terms

Cyber security is one of the defining elements of the security environment of the Slovak Republic and a subsystem of national security. At a state level, *it is a system* of continuous and planned increasing of political, legal, economic, security, defence and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organizational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of social and economic processes at an acceptable level of risks in cyber space.

The Slovak Republic still lacks a consistent formalized terminology in the area of cyber security. The word *cyber* and its other grammatical forms do not occur in any generally binding regulation nor in terminological dictionaries[2].

Definitions of the practically used terms in the cyber security area and definitions of key terms: *cyber security, cyber space, national cyber space* for the purposes of this Concept are specified in the Annex no. 1 to the Concept[3]. For the real performance of state administration in the area of cyber security and to understand the relationship between cyber security and the basic security areas of operation of the state[4], a legally binding definition of the meaning of these terms is of crucial importance[5]. The relation of cyber security to the basic security areas of operation of the state and the mutual relation between *cyber security* and *information security* are discussed in the following chapter of the Concept.

2.2 Basic Principles of Cyber Security

The field of cyber security must not be seen as an isolated problem of the Slovak Republic or an isolated problem of one or several elements of society. Due to its global nature, cyber security is a society-wide phenomenon. Cyber security must be based on a complex approach, requiring intense joint use of information and coordination of activities on both national and international levels. When building cyber security, it is necessary to pursue collaboration between the civilian and security units of the state, public and private sectors, as well as national and international institutions. Providing for an efficient and effective protection of cyber space must be ensured by relevant entities that are responsible for the infrastructures of individual sectors on a national level and by entities responsible for the operation of international infrastructures[6].

The Slovak Republic is fully in line with the principles of cyber security specified in the strategic document "Cybersecurity Strategy of the European Union"[7] as well as with the principles specified in the "Enhanced NATO Policy on Cyber Defence"[8].

---

2 *Website of the Ministry of Finance of the Slovak Republic.*

3 *The Annex is not a binding terminological dictionary for cyber security.*

4 *Basic security areas of operation of the state in the structure of the Report on Security of the Slovak Republic.*

5 *Article 2(2) of the Act no. 460/1992 Coll. the Constitution of the Slovak Republic: State bodies can act only on the basis of the Constitution, within its limits and to the extent and in a manner defined by law.*

6 *For example: Internet Corporation for Assigned Names and Numbers, ICANN; Internet Assigned Numbers Authority, IANA; Governmental Advisory Committee, GAC.*

7 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013).*

8 *Enhanced NATO Policy on Cyber Defence. 2014.*

Characteristic Features of Cyber Security

A significant feature of cyber security is the fact that individual components of cyber space have different owners, administrators, operators, as well as users. Failure to adhere to minimum security rules, protection methods and minimum security measures in the area of cyber security and the lack of unification thereof increases the level of vulnerability of the operated electronic information, communication, and control systems and in case of a cyber attack, it may even cause risks for a selected part of for the whole of cyber space.

Managing security incidents and events does not only depend on the capacities of the public sector but it is also significantly dependent on the constructive cooperation of actors active outside the public sector.

Cyber Security as a Component of the State's Security System

Insufficient protection and defence against security incidents creates space for rendering society itself vulnerable, with consequences throughout all social and economic processes, i.e. the state's basic security areas of operation (hereinafter referred to as the "security areas") may be seriously endangered:

- Security interests of the Slovak Republic in foreign and defence policy.
- Protection of constitutionality, public order, security of citizens and the state.
- Social stability of the state.
- Economic stability of the state.
- Protection of the environment.

Cyber security is perceived as a key component of state security. The basic components forming and implementing the security system of the Slovak Republic are, according to the law[9]: foreign policy, defence planning, civil emergency planning and coordination and intelligence services. Currently, a bill is being prepared that will recognise the protection of the national cyber space as another key component of the security system of the state.

Globalism and the importance of the impacts of potential cyber attacks require a conceptual and coordinated control of the protection and defence of cyber space.

Cyber Security and Information Security - Relations

For the purposes of this Concept, the definition of the terms cyber security and information security is based mostly on EU documents[10]. These documents imply that these are two mutually interconnected areas of problems, i.e. the security of the cyber environment and the security of the information environment, or cyber security and information security.

The information environment is one of the important real environments[11] within a specific framework of the socio-economic environment.

---

9 *Act no. 110/2004 Coll. on Operation of the Security Council of the Slovak Republic at Peace Times, as amended by the Act no. 319/2012 Coll.*

10 *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high joint level of network and information security. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013).*

11 *E.g..: social, work, legal, etc.*

Cyber space is limited by the use of electronics and of the electronic spectrum to create, store, modify, exchange, and use data by mutually dependent and interconnected networks.

Cyber security is a system tasked to provide the information environments of the state's socio-economic structures with secure, protected and adequately open cyberspace, i.e. to guarantee security in the electronic information, communication and control systems located in this environment, the security of the data stored, processed and transmitted in the systems and of the services provided by these systems.

The joint task of cyber and information security is to provide, in collaboration, for information safety, availability of systems and services, as well for the safety of the data transmitted by, processed by and/or stored in these systems in a specific socio-economic environment.

2.3 Current Situation in the Slovak Republic

The field of cyber security in the Slovak Republic has not been integrally and consistently regulated at a national strategic level. Some attention was paid to cyber security in the document "National Information Security Strategy of the Slovak Republic"[12] (hereinafter referred to as the "Strategy") and the subsequent "Action Plan for 2009 to 2013 for the National Information Security Strategy of the Slovak Republic"[13].

An overview of documents approved by the Government of the Slovak Republic in relation to the implementation of this Strategy as well as of other strategic and/or conceptual documents partially related to the area of protection of cyber space and/or cyber security in provided in Annex no. 2 to this Concept.

The Slovak Republic has adopted several regulations regulating the security of information and communication systems and information processed and/or transmitted thereby[14].

The "Reports on the Performance of Tasks of the National Information Security Strategy of the Slovak Republic and Tasks of the Action Plan for 2008 to 2013"[15] show that among the tasks of a non-legislative nature, positive results have been achieved in the area of information security mainly in the building of skills, education, prevention and readiness to managing computer security incidents, in the removal of the consequences thereof and the subsequent restoration of information systems in the framework of central state administration. The training of state administration specialists is carried out mostly at the Ministry of Finance of the Slovak Republic. Increasing awareness and education in the area of cyber and/or information security is not generally included in the educational system of the Slovak Republic (primary and secondary schools and universities) nor in the system of forming social awareness.

Education is not dealt with at the level of specialized majors but mostly by special courses at selected educational institutions. Differing levels of capacities and preparedness for cyber risks still exist. What is absent is an Centre of Excellence that would focus on questions related to cyber security.

The collaboration of the public sector with the private sector, academic institutions and civil society has not developed in the necessary scope and a framework of systematic, coordinated and efficient collaboration, mostly at a strategic level, is lacking.

---

12 The Government of the Slovak Republic approved the material (mat. no. ÚV-18175/2008) on 27 August 2008 by its Resolution no. 570/2008.

13 The Government of the Slovak Republic approved the material (mat. no. ÚV-30315/2009) on 19 January 2010 by its Resolution no. 46/2010.

14 E.g. Act no. 45/2011 Coll. on Critical Infrastructure defining the organization and powers of state administration bodies in the area of critical infrastructure, Act no. 351/2011 Coll. on Electronic Communications as amended.

15 http://www..informatizacia.sk/narodna-strategia-pre-ib/6783s.

Cyber threats are not generally seen as a sufficiently urgent problem. It is still necessary to focus attention on vulnerabilities that today's society faces more and more, to increase awareness also among the general public and to take steps to eliminate the threats and risks related to the use of modern information and communication technologies.

The most serious problem in the area of cyber security in the Slovak Republic is the fact that the protection of cyber space, or the cyber security of the Slovak Republic, is not yet explicitly and integrally regulated in valid law[16].

Existing capacities and mechanisms in the area of network and information security are no longer sufficient to keep the pace with a dynamically changing environment of threats and to provide a sufficiently high and, above all, legally effective, level of protection in all areas of the state's administration and of social life.

The Slovak Republic, as a member state of NATO and of the EU, also participates in the formulation of international strategic and conceptual documents, international policies and standards and must implement the adopted documents[17] and transfer them to national law. The Slovak Republic is active in international cooperation, with representatives in numerous international organizations as well as EU and NATO bodies. The Slovak Republic actively pursues its interests in this area. It regularly participates in cyber trainings (Cyber Coalition, Locked Shields, Cyber Europe and others), testing the abilities and reactions of the Slovak Republic to cyber attacks each year. A training entitled "SISE 2010 to 2013" has been coordinated on a national level. The Slovak Republic closely cooperates, without limitation, with the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (NATO CCD COE), the European Network and Information Security Agency (ENISA) and the recently created European Cybercrime Centre (EC3). In years 2013 – 2014, the National Security Authority has fully accepted the tasks of building NATO cyber defence and information security in the Slovak Republic within the Forces Targets 2013 defence planning.

2.4 Purpose of the Concept

The ***strategic goal*** of cyber security in the Slovak Republic is to achieve an open, secure, and protected national cyber space, i.e. building trust in the reliability and security of, above all, critical information and communication infrastructure, as well as building of certainty that this will perform its functions and serve national interests also in cases of cyber attacks.

Basing on the current situation in cyber security in the Slovak Republic, the ***goal of the Concept*** is to achieve a state where:

- Protection of national cyber space is a system operating conceptually, in a coordinated manner, efficiently, effectively, and on a legal basis.
- Security awareness of all components of society is systematically increasing.
- The private and academic sectors as well as civil society actively participate in the formulation and implementation of the policy of the Slovak Republic in the area of cyber security.
- Efficient collaboration is provided for both at national and international levels.
- The adopted measures are adequate and respect the protection of privacy and basic human rights and freedoms.

16 *See the conclusions of the reports on performance of tasks of the Strategy and Action Plan in Annex no. 3 hereto.*

17 *These include, without limitation, the NATO Policy on Cyber Defence, 2011; NATO Cyber Defence Action Plan; Enhanced NATO Policy on Cyber Defence, 2014; Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN (2013).*

3 Proposed Solution

Basing on the starting points, principles and goals defined in the previous chapter of the Concept, the proposed solution specified in this part defines the methods and measures for the Slovak Republic to achieve the target condition. It defines the method and tools to be used by the Slovak Republic to try to reduce the risks and threats coming from the cyber space, without restricting the benefits of the use thereof. These will further serve as the basis for the Action Plan for Implementation of the Cyber Security Concept of the Slovak Republic for 2015 – 2020 (hereinafter referred to as the "Action Plan") that will define specific tasks, including the material, time and financial plan for the implementation of the Concept.

The Concept considers the following to be the basic ***implementation tools*** of the above goal:

- A cyber security control system with a legal basis (institutional, regulatory and methodical framework), including specialized institutions and area of terminology.
- High culture of risk control, information exchange between private and public sectors and increasing capacities of actors.
- Systematic informing and a complex education system in the cyber security area.
- Cooperation and partnerships at national and international levels of all relevant entities from public, private and academic sectors and the civil society.
- Development of an internal market with cyber security products and services, especially using grants, EU funds and support for newly emerging projects or start-ups, as well as support for research, development and innovation of industrial and technological sources of cyber security.

The Concept proposes to adopt and solve, as priorities, the following seven key measures:

- **Measure 1:** Building an institutional framework for cyber security administration.
- **Measure 2:** Creating and adopting a legal framework for cyber security.
- **Measure 3:** Defining and applying basic mechanisms for securing the administration of cyber space.
- **Measure 4:** Supporting, preparing, and introducing a system of education in the area of cyber security.
- **Measure 5:** Defining and applying a risk control culture and a system of communication between the stakeholders.
- **Measure 6:** Active international collaboration.
- **Measure 7:** Supporting science and research in the area of cyber security.

3.1 Building an Institutional Framework for Cyber Security Administration

The Concept proposes the structure of cyber security administration as shown in Figure no. 1.

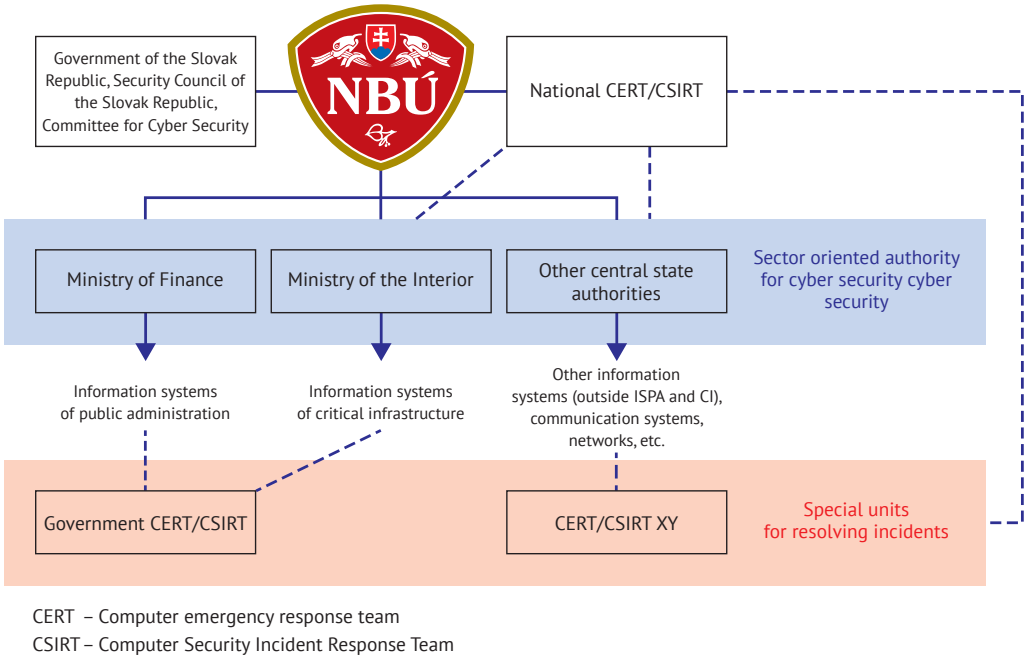


Figure no. 1 Proposed framework structure for managing cyber security

Cyber security at a national level belongs to the scope of powers of the relevant central state administration body, with competences and powers defined in general by the Competence Act and specifically by a special law (Cyber Security Act). The scope and method of the exercise of public authority in the area of cyber security by relevant central state administration bodies and other state bodies in the framework of specific material areas of administration of the state's socio-economic environment (hereinafter referred to as "material areas") will be defined by a special law (Cyber Security Act).

Complex provision for cyber security within individual material areas must be performed by the exercise of public authority and exercise of special activities. The Concept foresees that a National Incident Resolution Unit and several incident resolution units in material areas of special importance (hereinafter referred to as the "units") will be formed. To use human capacities rationally and use the technological equipment of the unit efficiently, the Concept foresees the formation of common units for other material areas; the National Incident Resolution Unit can hold the authority in certain material areas. The competences and authority of the National Incident Resolution Unit and of the units will be defined by the Cyber Security Act.

The Concept proposes the following framework definition of the powers and competences of public administration bodies in the area of cyber security at a central level:

Central state administration body for cyber security – the authority of an existing non-sectoral central state administration body[18] extended by another segment of state administration. The Concept recommends that the lawmaker entrusts this authority to the National Security Authority.

18 *I.e. a state body whose powers do not relate to a specific material area of administration of the state's socio-economic environment. E.g.: Office of Government of the SR, National Security Authority.*

Material scope: cyber security at a national level. In this authority, it also fulfils the duties of the "relevant national authority for the area of network and information system security" in the sense of Article 6 of the Proposal for a Directive[19].

Competences and responsibilities:

- Prepares the concept of state policy in the area of cyber security and directs its implementation in individual administration sectors,
- Prepares drafts of generally binding regulations and methodology, prepares rules for accrediting incident resolution units,
- Methodically directs the preparation of operating procedures for reactions to cyber threats at a national level,
- Coordinates the preparation of action plans for material areas with relevant central state administration bodies,
- Coordinates, monitors, controls and evaluates the execution of tasks in the area of cyber security at a national level,
- Serves as the national contact point for the EU and NATO in the area of cyber security/defence,
- Provides and coordinates the execution of tasks implied by international cooperation, represents the Slovak Republic internationally in the area of cyber security,
- Based on documents from other sectors, processes and prepares consolidated opinions for the Slovak Republic in the area of cyber security,
- Prepares Reports on the state of cyber security in the Slovak Republic and submits them for approval to the Cyber Security Committee of the Security Council of the Slovak Republic,
- In crisis management of the Slovak Republic, proposes and submits procedures for the case of cyber attacks,
- Continuously monitors the national cyber space and analyses potential and current threats,
- Performs state supervision over the activities of incident resolution units.

19 *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high joint level of network and information security in the Union.*

National Incident Resolution Unit (national CERT/CSIRT) – special unit with material scope in the area of cyber security at a national level, subordinated to the Central state authority for cyber security (also fulfils the tasks of the "computer emergency response team" under Article 7 of the Proposal for Directive[19]).

Competences and responsibilities:

- Systematically monitors the status of security and adherence to security standards in public administration information systems, continuously informing the Central state authority for cyber security,
- Provides and bears responsibility for coordinated incident resolution and/or coordinated reactions to cyber attacks,
- Sends early warnings, declares emergencies, announces and spreads information to relevant interested actors about risks and incidents,
- Ensures specialized training for incident resolution units and systematically manages training courses in the area of cyber security within its scope of powers,
- Ensures the execution of tasks implied by international collaboration within its scope of powers,
- Builds wide public awareness of the risks connected to activities performed on-line and organizes campaigns in the area of network and information security,
- Executes tasks of the incident resolution unit for certain material areas and/or on the basis of an authorization from a relevant central state administration authority.

Sector oriented authority for cyber security – organizational unit of existing central state authorities. Provides for cyber security within its material scope.

Competences and responsibilities:

- Responsible for the execution of state policies in the area of cyber security within its scope of powers,
- Ensures the exercise of state administration in the area of cyber security within its scope of powers,
- Provides collaboration to the Central state administration authority for cyber security when forming state policies in the area of cyber security,
- Cooperates with other sector oriented authorities for cyber security,
- Performs supervision over the activities of the sector oriented incident resolution unit,
- Ensures an increase in the level of security awareness and coordinates collaboration at all levels of cyber security control within its scope of powers.

Incident resolution unit (government CERT/CSIRT, CERT/CSIRT XY) – special unit of a central state administration authority – authority with material relevance of cyber security. The physical establishment of sectoral units in all sectors of administration is not foreseen. However, the following functionalities must be implemented in individual sectors of administration.[20]

20 *The conditions of establishing of incident resolution units and the scope of their authority, competences and duties, will be set by the Cyber Security Act.*

Competences and responsibilities:

- Systematically monitors the status of security and adherence to security standards of information systems in its material area,
- Ensures and bears responsibility for the execution of reactions to incidents and/or cyber attacks in its area of powers,
- Prepares operating procedures for reactions to incidents within its scope of powers and submits them for approval to the Central state administration authority for cyber security,
- Executes immediate warnings and early notification of cyber threats in its scope of powers,
- Assesses the reliability and security resistance levels of security mechanisms in relation to new security threats and risks in its scope of powers,
- Prepares regular reports on security incidents in its scope of powers,
- Ensures professional training and systematically administers training courses in the area of cyber security in its scope of powers,
- Cooperates with other incident resolution units.

Based on experience from international cooperation, membership in international organizations, as well as the experience of other countries, the efficient exercise of measures of cyber security requires wide-spectre cooperation not only between state administration and territorial self-administration but also with the academic sector, scientific institutions, and of the private sector. The Concept proposes the formation of a **formal platform for collaboration on a national level,** ensuring the participation of representatives of the corporate and academic sectors in the preparation and formulation of government decisions by submitting recommendations and/or opinions on the development and continuous improvement of the cyber security system of the Slovak Republic.

3.2 Creation and Adoption of a Legal Framework for Cyber Security

At present, the highest priority for a substantial increase in the efficiency and effectiveness of the protection of cyber space in the Slovak Republic is **the formal legal regulation of the cyber security control system.** For this purpose, it is necessary to:

1. Adopt a special *Cyber Security Act*, that will, without limitation:
    - Formally ensure the coordination of the formation and implementation of a unified state policy in cyber security,
    - Explicitly establish the material powers and competences of public authorities as well as the scope and method of exercise of their competences,
    - Explicitly define the powers and competences of other actors, as well as the scope and method of application thereof,
    - Establish duties for entities using information and communication technologies in cyber space,
    - Will guarantee the rights, legally protected interests of other legal entities and natural persons and will define their duties.
2. Establish binding *terminology and standards* for the area of cyber security.
3. In individual sectors, issue a *methodical guidance* for the practical application of the Act and of standards in the system of the sector's management and operation.

3.3 Development and Application of Basic Mechanisms Providing for the Administration of Cyber Space

To ensure specialized tasks in order to render cyber space resistant, the Concept identifies and proposes the application and development of the following basic mechanisms:

1. Decision-making and control mechanism – continuous cross-sectoral planning, organizing, coordination, implementation and control of measures aimed at minimizing cyber security threats and preventing their growth into crisis situations:

    - Preparing crisis plans for solving crisis situations,
    - Summarizing the needs and requirements necessary to solve identified threats and confronting them with the possibilities of the state, regions, legal entities and natural persons,
    - Designating the forces, resources and funds necessary for solving crisis situations.

2. Prevention mechanism – protective measures aimed at acting against crisis situations arising and to minimize potential risks implied mostly for information and technical means of communication:

    - National policy of behaviour in cyber space,
    - Specialized training of professionals in the area of information and communication technical means as well as strengthening the security awareness of inhabitants in the field of information and communication technologies,
    - Technical/technological support – available for the general public, corresponding to the required protection levels, including recommendations, measures and technical measures including adequate software, hardware and regime standards, the settings and updates thereof,
    - Intelligence activities aimed at the collection, centralisation and evaluation of intelligence information useful for prevention (e.g. intelligence information about cyber threats),
    - Collaboration with member states of the EU and NATO, the relevant bodies of these organizations and with partner states in order to continuously monitor, analyse and evaluate the security situation in cyber space, discover threats of crisis situations early and coordinate the adoption of preventive measures to eliminate such threats.

3. Reaction mechanism – measures aimed at a qualified and efficient reaction in the event of incidents and/or crisis situations that need to be taken in cases of ongoing attacks in order to fence off or counterwork the attack and prevent the attacker from causing damage:

    - Defensive activities aimed at preventing the attacker from performing and/or continuing in the cyber attack; this involves the activation of entities active when solving crisis situations and if necessary, an early warning for the public, taking measures aimed at stopping the escalation of the crisis situation and the creation of conditions for a return to a stabilized situation,
    - Offensive activities aimed at weakening and/or eliminating the cyber and even physical capacities of the attacker and to discourage the attacker from continuing in the attacks,
    - Intelligence activities aimed at supporting defensive and/or offensive activities (e.g. intelligence information about the cyber capacities of the attacker).

4. Restoration mechanism – rescue measures aimed at reducing the consequences of damage caused by cyber attacks and return to the original state:

   - Removal of the consequences of the crisis situation and return to a stabilized state,
   - Organizational, personnel, technological and other specific measures to avoid the re-occurrence of the crisis situation and/or threat.

The nature of the fight against cyber attacks implies the necessity to use all security mechanisms and tools with efficient cross-sectoral and international cooperation.

3.4 Support, Formulation and Implementation of an Education System in the Area of Cyber Security

The quality, efficiency and effectiveness of performance of measures and tasks in the area of cyber security depend substantially on the level of social awareness, education level of society, as well as of the abilities of the actors in the area. For this purpose, it is necessary to identify specific tasks of the Action Plan for the areas of:

1. Spreading knowledge and raising awareness.
2. General educational system in the Slovak Republic at the levels of:
   a. Primary education,
   b. Secondary education.
3. Specialized educational system at the levels of:
   a. Secondary education,
   b. University education,
   c. Experts.

3.5 Determination and Application of Risk Management Culture and Communication System Between Stakeholders

An efficient and secure system for on-line communication and the exchange of information between the entities of the control structure of cyber security as well as with other relevant actors in the national cyber space, with optimal setting of competences, is necessary to ensure its protection. This is why it is necessary, at national and sectoral levels and at the levels of key actors from the private sector:

- To set up control and executive structures optimally, with clearly defined powers and competences,
- To prepare and introduce relevant methodologies and standards,
- To implement relevant supporting information, communication and control systems as well as secure systems: exchange of information, early warning and coordinated reaction.

3.6 International Cooperation

Due to its global nature, cyber security requires an intense joint use of information and coordination of activities both at national and international levels. The Slovak Republic, as a member state of NATO and the EU, will participate in drawing up international strategic and conceptual documents, international policies and standards and will, at the same time, build the most efficient model of cooperation, exchange and joint use of information between CERT and CSIR-type offices. Besides active international collaboration in international organizations and structures, the Slovak Republic will also establish and develop bilateral collaboration with nations sharing identical values. The Slovak Republic will organize and participate in international cyber trainings and exercises.

3.7 Support of Science and Research in the Area of Cyber Security

In the framework of cooperation of the public sector with the private sector and the academic institutions, the Slovak Republic also intends to support the development of cooperation in research projects (including qualitative and quantitative research). It will support participation in national as well as European research projects and activities in the area of cyber security, stressing the use of funds from the Research and Innovations Operating Programme for the 2014 - 2020 programming period. Research activities in the area will be coordinated by the central state administration authority for cyber security.

The Slovak Republic also intends to support the private sector and academic institutions in the development and implementation of information and communication technologies aimed at the protection of cyber space and in the development thereof; stimulation of investments in the area will be a national priority.

4 Conclusions and Recommendations

To protect national cyber space, fulfil the undertakings of the Slovak Republic as a member state of the EU and NATO and to fulfil other international undertakings, on the basis of experience from other member states, in order to optimize the collaboration between public administration bodies, as well as between public administration and the private and academic sector and in the interest of removing duplicities, the Slovak Republic has decided to adopt a conceptual material for the area of cyber security at a national level in the form of this Concept.

The Concept is the basic and starting document for the subsequent formulation of regulations, standards, methodology, rules, security policies and other tools necessary to provide cyber security. Since it is a defining element of the security environment of the Slovak Republic and a subsystem of national security, it is necessary to evaluate and build it up continuously. The Slovak Republic perceives the area of cyber security as an important part of the everyday use of information and communication technologies; this is why it will stress the execution of measures aimed at securing it.

The Slovak Republic will regularly evaluate and assess international law, international treaties, as well as trends and standards in the field of cyber security and will implement these and apply them when adopting legislation in the area of cyber security. The Slovak Republic intends to actively participate in the preparation of law, standards and norms in the institutions of the EU, NATO and other international organizations.

On the basis of the adopted proposals of the Concept, it is recommended to prepare and submit to the sessions of the Security Council of the Slovak Republic and of the Government of the Slovak Republic:

1. **A draft Cyber Security Act** that will integrally cover the area of cyber security.

2. **A Proposal of an Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015 – 2020** that will determine a material, time and financial plan for the implementation of the Concept. This document will include a material, time and financial plan of tasks for the individual central state administration bodies in the scope of their powers and competences within the basic security areas of operation of the state. The implementation of these tasks will serve to achieve the fulfilment of measures of the Concept in the application of basic principles of cyber security. A framework proposal of tasks is included in Annex no. 4 to the Concept.

In order to define, stabilize and use unified terminology related to cyber security, it is recommended to:

3. **Discuss the terminology used in the Concept** in the Cross-sectoral Terminological Commission of the Security Council of the Slovak Republic and subsequently to publish it in the Terminological Dictionary of Crisis Management.

For non-confidential facts, similarly to the definitions in regulations for confidential facts, it is recommended to establish formally, in an adequate scope:

4. **Requirements for physical, building, personnel and information security, as well as conditions of security of technical and system resources and cipher protection of information.**

In order to create conditions for systematic collaboration between the public administration, academic institutions, scientific sector and the private sector on ensuring cyber security in the Slovak Republic, it is recommended to create, at a national level:

5. **A formal cooperation platform.**

List of annexes

Annex no. 1: Interpretation of selected practically used and key terms for the purposes of the Concept.

Annex no. 2: Documents approved by the Government of the Slovak Republic in relation to the implementation of the National Information Security Strategy of the Slovak Republic and other strategic and/or conceptual documents.

Annex no. 3: Conclusions of Reports on Performance of Tasks of the National Information Security Strategy of the Slovak Republic and the tasks of the action plan for 2008 to 2013.

Annex no. 4: Framework proposal for the tasks of the Action Plan for the Implementation of this Concept.

Annex no. 1: Interpretation of Selected Practically Used Terms

"Asset"[21] is anything of value for an individual, organization, or public administration.

"Asymmetric Threat"[22] is a threat resulting from the potential use of different means or methods to avoid and/or supress the strengths of the enemy while using their weaknesses to reach an inadequate result.

"Attack"[23] is an attempt to destroy, endanger, modify, put out, steal, or gain any benefit by unauthorized access and/or unauthorized use. It is the performance of an offensive action against a set target6.

"Critical Information and Communication Infrastructure"[21] is the set of systems, infrastructures, networks and services of information and communication technologies that would, if disturbed, damaged, or unavailable, seriously impact the operation of other sectors of critical infrastructure and of social functions of vital importance, including national, economic and public security.

"Critical Infrastructure"[21] means the systems and services whose failure and/or incorrect operation would significantly impact the security of the state, its economy, public administration and as a consequence, the coverage of basic life needs of the population. The following 5 sectors are often defined in critical infrastructure: sector of information and communication technologies, energy sector, banking and finance sector, physical distribution (i.e. mainly transport systems) and sector of services significant for people.

"Cyber Space"[24] is a virtual space without borders, comprising worldwide interconnected networks of hardware, software and data.

"Cyber Security"[24] is a set of legal, organizational and technical measures protecting cyber space.

"Cyber Attack"[25] is an attack against an ICT infrastructure in order to damage it, destroy it, obtain sensitive or strategically important information, or influence the decision-making processes of the victim. Cyber attacks influence all operating domains and are most frequently used in the context of those with political and/or military motivation.

"Cyber Defence"[25] is a set of active and passive measures aimed at prevention of cyber attacks and mitigation of their consequences. Also the resistance of an entity against attack and the ability of efficient defence.

"Incident"[21] in the environment of information and communication technologies (hereinafter referred to as "ICT") means each circumstance and/or event that is normally linked to outage of a network, services, or reduction of the quality thereof.

"Incident Resolution"[26] means all procedures supporting the analysis, monitoring and reactions to incidents.

"Information Environment" is the sum of individuals, organizations and systems that collect, process, distribute and/or work with information.

"Information Security"[23] is a set of measures to ensure the integrity, confidentiality and accessibility of information, networks and information and communications systems.

---

21 *Interpretation dictionary of Cyber Security, Second updated edition under the auspices of the National Cyber Security Centre of the Czech Republic and the National Security Authority of the Czech Republic, © Jirásek, Novák, Požár, Praha 2013.*

22 *Dictionary of Military Terminology of the Armed Forces of the Slovak Republic, Bratislava, 2007.*

23 *ISO IEC 27000:2014 Information technology-Security techniques – Information security management systems – Overview and vocabulary*

24 *https://ccdcoe.org/cyber-definitions.html*

25 *National Security Authority.*

26 *Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security in the Union, COM (2013) 48 FINAL, Brussels, 2013.*

"Infrastructure" generally means the group of mutually interconnected components that provide a framework support to the whole, i.e. mutually dependent networks and systems generally interconnected at various levels, including industries, institutions and distribution capacities that provide a flow of products and services. These represent the material and technical facilities of the state, i.e. sectors carrying out economic and social system functions, such as energy, transportation, etc.

"Security Event"[21] is an event that may cause and/or lead to a violation of information systems and technologies and rules of security policy.

"Security Incident"[21] is a violation of an imminent threat of violation of security policies, security rules, or standard security rules of operation of an information and communications system or of a network.

"Security Measure"[21] is a protective measure ensuring security requirements are put into place on the system. These may be of different natures (physical protection of a device and information, personnel security – staff check, organizational measures – operating rules, etc.).

"Security of Information System" means the ability of a network or of an information and communication system to resist, at a certain reliability level, random events and/or intentional actions that endanger the availability, integrity and confidentiality of the saved and/or transmitted data and/or of related services provided by the network and information system and/or accessible using the network and the information system.

"Security Threat"[21] is a potential cause of an unwanted event that may result in damage to system and its assets, e.g. destroying, unwanted accessibility, modification, unavailability of services, etc.

"Security Vulnerability"[21] is an intentional error or an unintentional defect and/or error of software or hardware of infrastructure facilities that may be misused by potential attackers for damaging activities. These vulnerabilities are either known and published but not yet treated by the producer or hidden and non-discovered.

"System Resistance"[21] the ability of a system to resist threats and face impacts of outages.

"Risk"[26] means any circumstance and/or event that has a potentially unfavourable impact on security.

"Vulnerability"[21] is a weak point of an asset or of a control that can be exploited by a threat.

Interpretation of Key Terms for the Purposes of the Concept

Cyber Security in General is the ability of any electronic communications network, electronic information and/or control system to resist, at a certain reliability level, random events and/or damaging activities that may negatively influence the integrity, faithfulness, confidentiality and availability of the stored, processed and/or transmitted data and/or services provided by the network or by an information or control system and thereby to disrupt and/or negatively influence the operability of, without limitation, one of the sectors of critical infrastructure[27] and/or one of the basic security areas of operation of the state.

Cyber Security from a Process Viewpoint, at a state level, is the system of continuous and planned increase in political, legal, economic, security, defence and educational awareness that includes increasing the efficiency of the adopted and applied technical and organizational measures of risk management in cyber space in order to transform it into a trustworthy environment that will provide for safe operation of social and economic processes while ensuring an acceptable level of risks in cyber space[28].

Cyber space is a virtual space without borders, seen as a global interactive domain in an information environment that is characterised by the use of the electronic and electromagnetic spectre for the creation, storage, modification and exchange of data and use of services. Cyber space also means a combined phenomenon of global connection, de-centralized and continuously growing electronic information, communication and control systems, as well of the interconnection of social and economic processes in the form of data and information using these systems, including the data stored and/or processed therein.

National Cyber Space of the Slovak Republic includes the parts of the above systems of cyber space that are located in the territory of the Slovak Republic as well as other systems of cyber space that contain data and information aimed at the Slovak Republic and/or influencing the Slovak Republic[29].

Information Environment means a set of individuals, organizations and systems that collect, process, spread, or work with information irrespective of whether the information is in physical form, in audio form, or in electronic form.

Information Security means: a set and application of security measures and procedures[30] serving in the framework of a specific information environment, to protect information from impairment/loss, or compromising (loss of confidentiality, integrity and other characteristics such as authenticity, trustworthiness, non-deniability and reliability) and to preserve the availability of information and the ability to work therewith in the scope of assigned authorizations.

---

27 *Act no. 45/2011 Coll. on Critical Infrastructure as amended, states in Art.2(c) that "critical infrastructure" is a system divided into sectors and elements. The meaning of these components is defined in Art. 2(a) and 2(b) of the same Act.*

28 *The term cyber security should also be understood as dedicated mechanisms, defined policies, as well as processes tasked to protect systems and data from cyber threats and/or attacks.*

29 *The definition of the contents of this term is of substantial importance from the formal law aspect as the jurisdiction of the Slovak Republic cannot be applied in the framework of cross-border, i.e. global cyber space, it must be limited to a part thereof, i.e. to the National Cyber Space.*

30 *Security project according to the ISO 27000 standard.*

Annex no. 2: Documents approved by the Government of the Slovak Republic in relation to the implementation of the National Information Security Strategy of the Slovak Republic and other strategic and/or conceptual documents

In relation to the implementation of the Strategy, the Government of the Slovak Republic has approved, by resolutions:

- No. 479/2009 Organizational, personnel, material, technical and financial coverage for the creation of a specialized unit for computer incident resolution (CSIRT.SK),
- No. 46/2010 Draft Action Plan for 2009 to 2013 to the National Information Security Strategy of the Slovak Republic
- No. 136/2010 Legal intention of the Information Security Act[31],
- No. 391/2009 Education system in the area of information security in the Slovak Republic.

On the basis of item B.4. of the Resolution of the Government of the Slovak Republic no. 570/2008, the Ministry of Finance of the Slovak Republic has in each year between 2010 and 2014 prepared and submitted to the Government a Report on the performance of tasks of the Strategy and the Action Plan[32].

Other strategic and/or conceptual documents with contents partially dedicated to the problems of protection of cyber space and/or cyber security are:

- Concept of Critical Infrastructure in the Slovak Republic and Methods of Its Protection and Defence, approved by the Resolution of the Government of the Slovak Republic no. 120/2007.
- National Policy for Electronic Communications for 2009 - 2013, approved by the Resolution of the Government of the Slovak Republic no. 360/2009.
- Reports on Performance of Tasks of the Action Plan for the National Information Security Strategy of the Slovak Republic for 2009 to 2013, materials acknowledged by the Government of the Slovak Republic each year from 2010 to 2014.
- White Paper on Defence of the Slovak Republic, approved by the Resolution of the Government of the Slovak Republic no. 326/2013.

Report on Security of the Slovak Republic for 2012, approved by the Resolution of the Government of the Slovak Republic no. 325/2013.

- Integrated Infrastructure Operating Programme for 2014 - 2020, approved by a Resolution of the Government of the Slovak Republic no. 171/2014.
- Preparing the Slovak Republic for the performance of tasks in the area of cyber defence, implied by the goals of abilities of the Slovak Republic, approved by Government Resolution no. 497/2014.
- Report on the Security of the Slovak Republic for 2013, approved by a Resolution of the Government of the Slovak Republic no. 276/2014.[1 2]

31 *Under item B.3. of Government Resolution no. 570/2008, a proposal of legal intention of the Public Administration Information Security Act was to be submitted to the Government of the Slovak Republic.*

32 *http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s*

Annex no. 3: Conclusions of Reports on the Performance of Tasks of the National Information Security Strategy in the Slovak Republic and tasks of the Action Plan for 2008 to 2013

2009 Report

Contains no conclusion. The end of the Report contains the "Proposal of performance of tasks for 2009"

2010 Report

By comparing the results of monitoring to the results of inspections it can be stated that identical problematic areas and critical factors have been identified. The process of information security management has systematic deficiencies in the area of the preparation of crisis plans, the transfer of competences and crisis management. To remove deficiencies more efficiently, it is necessary to speed up the introduction of systematic education in the area at all levels and apply a sanction mechanism for violations of Act no. 275/2006 Coll. on Public Administration Information Systems and on the modification and amendment of other acts as amended thoroughly, including its implementing regulations.

2011 Report

The main task in the area of IB is to create a single platform for building an information society, built on a legal basis, providing adequate protection and trustworthiness to the digital space of Slovakia.

To reach and maintain the required condition of IB, it is necessary to solve, in 2011, the priority tasks, especially in the area of law, knowledge standards for IB and the coordination of exercises for cases of reaction and restoration after security incidents at a national level and related activities.

2012 Report

The main task in the area of IB is to create a unified platform of building IB, based on a legal basis, providing adequate protection and trustworthiness to the digital space of the Slovak Republic. To reach and maintain the required condition of IB it is necessary, during the coming period, to solve the priority tasks especially in the area of law, knowledge standards for IB and coordination and exercises for cases of reaction and restoration after security incidents at national and international level and related activities.

2013 Report

The main task in the area of IB is to create a unified platform of building IB, based on a legal basis, providing adequate protection and trustworthiness to the digital space of the Slovak Republic. To reach and maintain the required condition of IB it is necessary, during the coming period, to solve the priority tasks especially in the area of law, knowledge standards for IB and coordination and exercises for cases of reaction and restoration after security incidents at national and international level and related activities. These activities are fully harmonized with the goals of the proposal for "Directive concerning measures to ensure a high common level of network and information security in the Union"; it will be necessary to create a legal base for the missing competences and duties of the already formed "CSIRT. SK" unit; this is a task for the Ministry of Finance of the Slovak Republic. The purpose is to bring the unit at least to the level of similar units in developed EU member states. The transposal of the directive in the territory of the Slovak Republic will be performed in the prepared Information Security Act that will also require amending other related generally binding regulations.

2014 Report

When comparing the status for the period of 2013 to the previous period, one can state that minor improvements in several areas compared to the previous period fail to reflect the possibilities for improvement. Despite improvements in certain areas, stagnation and/or worsening of situation was seen in most areas. This negative phenomenon can be explained by failure to adhere to the existing regulatory framework, lack of qualified staff and generally the low security awareness of entities active in the area of IB in public administration.

Improvement of the situation in the field can be expected after the introduction of legal and organizational measures, standardized procedures and control mechanisms. This applies, above all, to the introduction of mandatory classification of information and information systems of public administration and the subsequent introduction of minimum security measures for their protection, also defining legal responsibility for the suppliers of these services. Another condition for the improvement of the overall situation is the introduction of the process of IB management in organizations, risk management and without doubt, an increase in security awareness and skills of personnel. Preparing the environment for the introduction of the required measures will require legal changes that were defined in the legal intention of the Information Security Act approved by the Government; its intention will also be reflected in the prepared Information Security Act.

Annex no. 4: Framework Proposal of Tasks of the Action Plan for the Implementation of the Concept

Measure 1:
Creation of an institutional framework for cyber security control

Responsible authority: Office of the Government

Tasks:

1. Prepare a draft of an amendment to the Competence Act referring the competence of the central state authority in the area of cyber security to the National Security Authority.

2. Prepare a draft for the creation of a formal platform for cooperation in the area of cyber security at a national level.

Collaboration: central state authorities

Tasks:

3. Form personnel and material and technical conditions for the exercise of competences of the sector oriented authority for cyber security within its scope of powers.

4. Form personnel and material and technical conditions for the exercise of competences of the incident resolution unit.

5. Prepare draft methodological guidelines for the exercise of competences of the incident resolution unit.

Measure 2:
Creation and adoption of legal framework of cyber security

Sponsor: Central state authority for cyber security

Tasks:

1. Form personnel and material and technical conditions for the exercise of competences of the central state authority for cyber security.

2. Form personnel and material and technical conditions for the exercise of competences of the National Incident Resolution Unit.

3. Prepare draft methodological guidelines for the exercise of competences of the National Incident Resolution Unit.

4. Prepare a draft terminological dictionary for the area of cyber security.

5. Prepare a draft of the Cyber Security Act.

6. Prepare a draft of standards for cyber security.

Collaboration: central state authorities

Tasks:

7. Submit specific proposals and work actively in working groups created by the sponsor.

8. Prepare a draft of provisions of the Cyber Security Act related to the specifics of the administered sector from a cyber security viewpoint.

9. Provide active expert collaboration when preparing drafts of: terminological dictionary, Cyber Security Act, standards for cyber security. Submit a draft of methodical guidelines for the exercise of competences of the sectoral incident resolution unit to the sponsor.

Measure 3:
Developing and applying basic mechanisms for securing the administration of cyber space

Sponsor: Central state authority for cyber security

Tasks:

10. Develop basic mechanisms for securing the administration of cyber space and ensure the application thereof at a national level.

Collaboration: central state authorities Tasks:

11. Develop basic mechanisms for securing the administration of cyber space and ensure the application thereof at the level of the relevant administered area.

Measure 4:
Support, development and implementation of an education system in the area of cyber security

Sponsor: Ministry of Education, Science, Research and Sport

Tasks:

1. Prepare a draft for the full coverage of education in the area of cyber security in the framework of the systems of:
    a. General education in the Slovak Republic at the levels of:
        - Primary education,
        - Secondary education,
    b. Specialized education at the levels of:
        - Secondary education,
        - University education,
        - Experts.

Collaboration: central state authorities

Tasks:

2. Submit a proposal for the coverage of the specific needs of the sector to the Ministry of Education, Science, Research and Sport.

Sponsor: Ministry of Culture

Tasks:

3. Prepare a draft for the provision of the systematic spreading of knowledge in the area of cyber security.

Measure 5:
Setting and application of a culture of management of risk and system communication among stakeholders

Sponsor: Central state authority for cyber security

Tasks:

1. Design and create managing and executive structures with clearly defined powers, competences and set rules of mutual communication and collaboration at a national level.

2. Prepare and implement a project for a system of on-line risk management and communication between actors providing for the operability of systems and services operating in national cyber space as well as its protection and security (secure systems of: exchange of information, early warning and coordinated reaction).

3. Prepare and implement a project for a system of on-line reporting and resolving incidents including the users of systems and services within national cyber space.

4. Prepare and implement a project for the administration and provided services of registers: identifying actors, their scopes of powers, competences, provided services and other relevant data.

Collaboration: central state authorities

Tasks:

5. Design and create managing and executive structures with clearly defined powers, competences and established rules of mutual communication and collaboration at the level of the administered material area.

6. Specify the requirements for the systems listed in sections 2 and 3 of this Measure.

7. In the necessary scope, provide collaboration during individual phases of the design and implementation of the said systems.

Cyber Security Concept of the Slovak Republic

for 2015 - 2020