REPUBLIC OF SLOVENIA

CYBER SECURITY STRATEGY

ESTABLISHING A SYSTEM TO ENSURE A HIGH LEVEL OF CYBER SECURITY

DIGITAL SLOVENIA

Document Info

Title	Cyber Security Strategy
Date	February 2016
Participants in document preparation:	• Agency for Communication Networks and Services of the Republic of Slovenia • Energy Agency of the Republic of Slovenia • Ministry of Defence • Ministry of Economic Development and Technology • Ministry of Education, Science, and Sport • Ministry of Finance • Ministry of Foreign Affairs • Ministry of Health • Ministry of Infrastructure • Ministry of Public Administration • Ministry of the Interior • Ministry of the Interior –The Police • National Security Council • Office of the Government of the Republic of Slovenia for the Protection of Classified Information • Slovenian Computer Emergency Response Team (SI-CERT) • Slovenian Intelligence and Security Agency

Index

Purpose and summary

Slovenia's cyber security strategy will improve the country's cyber security assurance system, while also systematically regulating this area. Strengthening the overall system is necessary because of the ever-growing importance of cyber security for the smooth functioning of the systems the whole society depends on. Moreover, the state is encouraged and bound to do so by national and international strategic documents. An efficient cyber security assurance system is not and cannot be cheap, but it is incomparably cheaper than fixing any consequences that might arise as a result of security incidents if such systems were missing.

The strategy comprises an overview of the situation in those areas that are relevant for cyber security assurance, outlining the vision and setting objectives. It further defines the areas where it will be implemented, as well as the risks occurring in cyberspace. The strategy proposes the way the cyber security assurance system should be organised, and the measures necessary for achieving the set objectives.

1 Introduction

In modern world, the use of information systems and networks is constantly increasing, and therefore the importance of these systems for the successful development of economic and non-commercial activities, as well as the life and welfare of the society as a whole, is also increasing. Network and information security contributes to strengthening important societal values and objectives in the society, such as human rights and fundamental freedoms, democracy, the rule of law, and economic and political stability.

On the one hand, the increasingly rapid development of information and communication technologies (ICT) brings benefits to modern society, while on the other it gives rise to ever new and technologically more sophisticated cyber threats. The trend in the use of ICT for political, economic and military supremacy is becoming more and more pronounced. Undoubtedly, cyber attacks are among the most significant security threats to the modern world, and therefore, cyber security has become an important, integral part of national security.

In order to strengthen the cyber security assurance system, the state is encouraged and bound to adopt strategic documents at the national and international levels. This issue is addressed in the Resolution on the National Security Strategy of the Republic of Slovenia[1], the Cyber Security Strategy of the European Union "Open, safe and secure cyberspace"[2], and Draft Directive on measures to ensure a common high level of network and information security across the Union[3].

This strategy will help Slovenia define its measures for establishing a national cyber security system that will facilitate a rapid response to security threats and will serve to effectively protect the ICT infrastructure and information systems, thus ensuring the continuous operation of both public and private sectors, and, in particular, the key functions of the state and society in all security situations. Ensuring the security of cyberspace[4] will be balanced with the interests of ensuring safety and economic viability as well as human rights and fundamental freedoms.

[1] Resolution on National Security Strategy of the Republic of Slovenia. Uradni list RS (online), 2010, No. 27/2010, point 5.3.5 Responding to cyber threats and misuse of information technologies and systems. Available at: https://www.uradni-list.si/1/content? id=97018.

[2] Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace. Digital Agenda for Europe - A Europe 2020 Initiative [online], 2013. Available at: http://ec.europa.eu/digital-agenda/en/news/eu-cyber security-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[3] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. Digital Agenda for Europe - A Europe 2020 Initiative [online], 2013. Available at: http://ec.europa.eu/digital-agenda/en/news/eu-cyber security-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[4] The term cyberspace covers the information technology network, telecommunication networks and computer processing systems.

DEFINITION OF CYBER SECURITY[5]

Cyber security is generally defined as:

- a range of activities and other measures, both technical and non-technical, intended to protect computers, computer networks, hard- and software and the information stored and processed therein, including programmes and data as well as other cyberspace elements, from all threats, including threats to national security;
- the level of protection provided by these activities and measures;
- joint professional endeavours, including research and development to implement and improve these measures and increase their quality.

2 Analysis of the present situation

In Slovenia, there have already been a few proposals for systemic regulation of cyber security, however, their implementation never took place. Nevertheless, it became clear that the country needs a cyber security strategy that would join and direct the efforts of all stakeholders toward strengthening and systematically regulating this important area.

Currently, the operational capacities to respond to cyber threats are distributed among SI-CERT[6] as the national response centre for network incidents, the Information Security Sector within the IT Directorate at the Ministry of Public Administration, the Ministry of Defence for defence system and protection against natural and other disasters, Slovenian Intelligence and Security Agency (SOVA) in counter-intelligence activities, and the Police within its IT and telecommunications Office and the Criminal Police Directorate, mainly in the Centre for Computer Investigations with the capacities to combat cybercrime. Apart from the Police, which in the past five years has improved its capacities for investigating and preventing cybercrime, all other bodies lack personnel, material and technical resources, and organisation. Despite the shortcomings, the capacities at the operational level do exist though a coordination body that would link the concerned stakeholders at the strategic level is missing.

[5] Dunn, M. A Comparative Analysis of Cyber security Initiatives Worldwide. V: ITU WSIS Thematic Meeting on Cyber security [online], 2005, p. 4. Available at: https://www.itu.int/osg/spu/cyber security/docs/Background_Paper_Comparative_Analysis_Cyber security_Initiatives_Worldwide.pdf.

[6] Slovenian Computer Emergency Response Team (SI-CERT) is a national response centre for dealing with incidents in electronic network and information security, which has been operating within the public institute ARNES since 1995. It coordinates incident resolution, provides technical advice in the event of intrusions, infections with computer viruses and other abuses, and issues warnings to network administrators and general public on the current threats to electronic networks. Currently, it also performs the tasks of Government's centre for responding to network indigents (SIGOV-CERT) and assists in the establishment of an independent centre that will be responsible for protecting the IT infrastructure of the state administration. SI-CERT is a member of the Forum of Incident Response and Security Teams (FIRST), a member of the group of national response centres at CERT/CC, a member of a work group of the European response centres TF-CSIRT, and is accredited Trusted Introducer. SI-CERT is the Slovenian contact point for the security authority of the General Secretariat of the EU Council and the national information point for the IMPACT programme of the International Telecommunication Union (ITU).

According to SI-CERT data[7], 2060 incidents were handled in Slovenia in 2014, which is almost a 6.4-fold increase with respect to 2008. The increasing trend regarding the above-mentioned deficiencies of the cyber security assurance system raises concern.

Cooperation of stakeholders in cyber security assurance is not formally regulated, however, response centres cooperate informally, unless there is a legal basis for it[8]. This includes providing information about incidents and help in their resolution, the exchange of experience or the use of existing capacities. An opportunity to establish cooperation is found, inter alia, joint participations in the implementation of international cyber security exercises, organised by the European Network and Information Security Agency (ENISA)[9]. Thus, such cooperation has already been established with some banks, telecommunication providers and electricity distributors.

There are two awareness-raising projects: since 2011, SI-CERT has worked to raise national awareness and holding the educational program "Safe on the Internet"[10]. The project's key objective, which is targeted at the general Slovenian public, and with a specific set of content also at small enterprises, craftsmen and sole proprietors, is to raise the awareness on the safe use of the Internet. The project, which is financed by the Ministry of Education, Science and Sport, is also participating in the campaigns of the European month of cyber security.

Within the framework of the Centre for Safer Internet, which is run by a consortium consisting of the Faculty of Social Sciences, ARNES, Slovenian Association of Friends of Youth and the Youth Information and Counselling Centre of Slovenia - MISSS [11] and funded by the Directorate-General Connect of the European Commission and the Ministry of Education, Science and Sport, SAFE.Si [12], TOM Telephone and the Web Eye projects are being carried out. The SAFE.SI program operates as a national point for raising awareness among children and adolescents about the safe use of the Internet and mobile devices. The TOM Telephone program also informs children and adolescents about the safe use of the Internet and mobile devices. Web Eye is an online reporting point, which – in partnership with the police, prosecution, Ombudsman for Human Rights, Internet service providers, public and other interested governmental and non-governmental organisations – allows anonymous reporting of material allegedly containing instances of the sexual abuse of a minor and hate speech on the Internet, and raises awareness on the problem of illegal web content.

In the education sector, IT or cyber security is included in the higher school study programme at the Faculty for Security Studies of the University of Maribor, and in the curricula of study programmes at the Faculty of Computer and Information Science and the Faculty of Social Sciences of the University of Ljubljana, at the Faculty of Electrical Engineering and Computer Science of the University of Maribor, the Faculty of Health Sciences of the University of Primorska, the Faculty of Information

[7] The data for 2014 and the reports for past years are available at https://www.cert.si.
[8] E.g., Article 81 of the Electronic Communications Act sets out the procedure of information exchange between AKOS and SI-CERT at the breach of security or integrity. Electronic Communications Act. In: Uradni list RS, 2012, No.109/2012, Article 81. Available at: http://www.uradni-list.si/1/content?id=111442.
[9] European Union Agency for Network and Information Security (ENISA)
[10] https://www.varninainternetu.si/
[11] Youth Information and Counselling Centre of Slovenia.
[12] http://safe.si/

Studies of Novo mesto, and the licensed independent higher education institution GEA College; as part of the corporate security subject it is also included in the study programs at some other higher education institutions. No subject in this area is taught at the primary and secondary school levels.

In accordance with its abilities, Slovenia participates in international cyber security exercises. In Cyber Europe exercises, organised by ENISA, in 2010 Slovenia took part as an observer and in 2012 and 2014 as an active participant. Furthermore, from 2013 on, it actively participates in Cyber Coalition exercises within NATO. Participation in these exercises proved to be a good opportunity to check the capacities for cyber security assurance at the national level, as well as to exchange experience and establish new connections between stakeholders. National cyber security exercise has not yet been carried out.

3 Vision

Establishing a comprehensive cyber security system as an important integral factor of national security will contribute to ensuring an open, safe and secure cyberspace, which will make the basis for smooth functioning of infrastructure, important for state bodies' operations as well as for the life of each individual.

By 2020, Slovenia will establish an effective cyber security assurance system, which will prevent and also eliminate the consequences of security incidents. This objective comprises eight sub-objectives:

1. strengthening and systemic regulation of the national cyber security assurance system;
2. the safety of citizens in cyberspace;
3. cyber security in the economy;
4. ensuring the operation of critical infrastructure in the sector of ICT support;
5. cyber security to ensure public security and combat cyber crime;
6. development of cyber defence capabilities;
7. ensuring the safe operation and availability of key IC systems in the event of major natural and other disasters;
8. strengthening national cyber security through international cooperation.

4 Cyberspace risks

In a modern society, practically all social activities depend on ICT systems, and with further development this dependence is likely to increase. Systems interconnectivity means that the vulnerability of one may affect the functioning of the other. As it is impossible to ensure complete security against cyber attacks, abuse, fraud, human and technical errors, and other influences, the approach used in determining the priority of a particular threat should be based on risk assessment.

In recent years[13], an increase in the number of security incidents, advanced targeted attacks, exposure of ICT infrastructure and the abuse thereof for implementing distributed denial-of-service[14]

[13] SI_CERT reports on the network security for years 2011, 2012, 2013 and 2014. Available at: https://www.cert.si.

have been noted. Individuals are exposed to various online frauds, attempts of abuse of electronic banking services and malicious code.

4.1 Technological Development

ICT develops extremely quickly, which indeed facilitates new innovative use , new business models and a variety of development opportunities, while it also requires rapid adaptation of the legislative and other social frameworks. Development guidelines suggest the implementation of cloud computing, data-guided economy and mass data, the Internet of Things and innovative collaborative business models based on them, where the limits of control and accountability for the protection of personal and other data are blurred or at least poorly defined. In cloud computing, in addition to ensuring safety and privacy, the quality of service can be questionable as well, since it is based on a chain of the mutual trust of all stakeholders that form the cloud, rather than on the assessment of the cloud as a whole. The ubiquitous mobile networks, the Internet of Things and mass data will increase exposure to security threats at different levels, which cannot be resolved without a systemic approach to risk management and a sufficiently high level of cyber security assurance.

4.2 The Internet

Considering the important fact that the Internet supports the operation of information and communication systems in many areas, it must be addressed accordingly and, being a key support system, also must be suitably protected. The Internet is exposed to risks posed by humans, natural and other disasters, and technical failures. Special attention should be given to the legislative and regulatory framework that addresses issues related to the protection of critical infrastructure in the IC support sector.

4.3 Cyber crime

The European Agenda on Security declares cyber crime to be one of the three threats to European security. With the increasing growth of widespread ICT use cyber crime, which includes a wide range of activities, is also on the rise. On the one hand it includes offenses related to intrusions of privacy, identity theft, obtaining information about individuals and legal entities for the purpose of extortion, fraud and online scams, dissemination of child pornography, digital piracy, economic espionage, money laundering, and counterfeiting, while on the other hand, it includes criminal offences related to attempts to obstruct the functioning of the Internet, ranging from mass-sending of unsolicited e-mails and implementation of distributed denial-of-services, to cyber terrorism, which may cause malfunctions of IC infrastructure and systems and may be as a result in some cases even life-threatening. Means and methods used in cyber crime are also used in more traditional forms of crime.

[14] DDoS (Distributed Denial-of-Service)

4.4 Intelligence

Society's overbearing dependence on ICT has increased the risks associated with the activities of foreign intelligence services. Various state or non-state stakeholders may exploit cyberspace to achieve their objectives, particularly by carrying out cyber-intelligence operations, which my in certain segments jeopardize the political, security and economic interests of the Republic of Slovenia.

4.5 Changes of the security environment

Malicious hacker intrusions into the information systems of state administration or state bodies also pose a security risk. Malicious activity against the cyber security of critical infrastructure represents a form of asymmetric warfare. Such activity is all the more dangerous in connection with increasingly organised international terrorist networks.

4.6 Intrusions of privacy

In an information society, individuals' privacy increasingly comes under attack, as it must be aligned with interests regarding retrieval, processing and storage of personal data by different companies for commercial purposes, as well as by state authorities. It is expected that with the increasing terrorist threats and the implementation of measures to prevent them trends towards greater control and, consequently, the restriction of individuals' privacy in the cyberspace will also be on the increase.

5 Identification of stakeholders

Public and private sector organisations participate in the cyber security system. Apart from the central coordination of the national cyber security assurance system and all the national response centres, an important role is played by the Electronic Communications Networks and Services Agency of the Republic of Slovenia (AKOS), telecom operators and telecommunication infrastructure administrators, information society service providers, academic and research community (some faculties and research organisations), occupational (chambers of commerce and industry) and professional associations (Slovenian associations and sections of international association in the area of information and communication technologies and cyber security), and software vendors that provide support to national authorities.

In a broader sense, stakeholders in cyber security assurance in Slovenia also include relevant organisations abroad, especially when these are cooperating with Slovenian stakeholders in response to security incidents. In this respect, partners within the EU and NATO are particularly important.

6 The establishment of a comprehensive cyber security system and clear governance structure

Successful high-level cyber security assurance requires the effective use of existing resources and appropriate multi-level organisation. Slovenia will set up central coordination of the national cyber security assurance system and provide conditions for its stable operation. This coordination body will

coordinate the cyber security assurance capabilities at the strategic level to ensure cyber security in the country at lower levels, and will represent a single point of contact for international cooperation. The organisation form of coordination functions will be determined by the Government of the Republic of Slovenia.

At the operational level of cyber security assurance, SI-CERT will operate with its capabilities at the national level, the Ministry of Defence in the field of defence and protection against natural and other disasters, the police in ensuring cyber security in the context of public safety and the fight against cyber crime, SOVA in counter intelligence, and the emergent SIGOV-CERT in public administration.

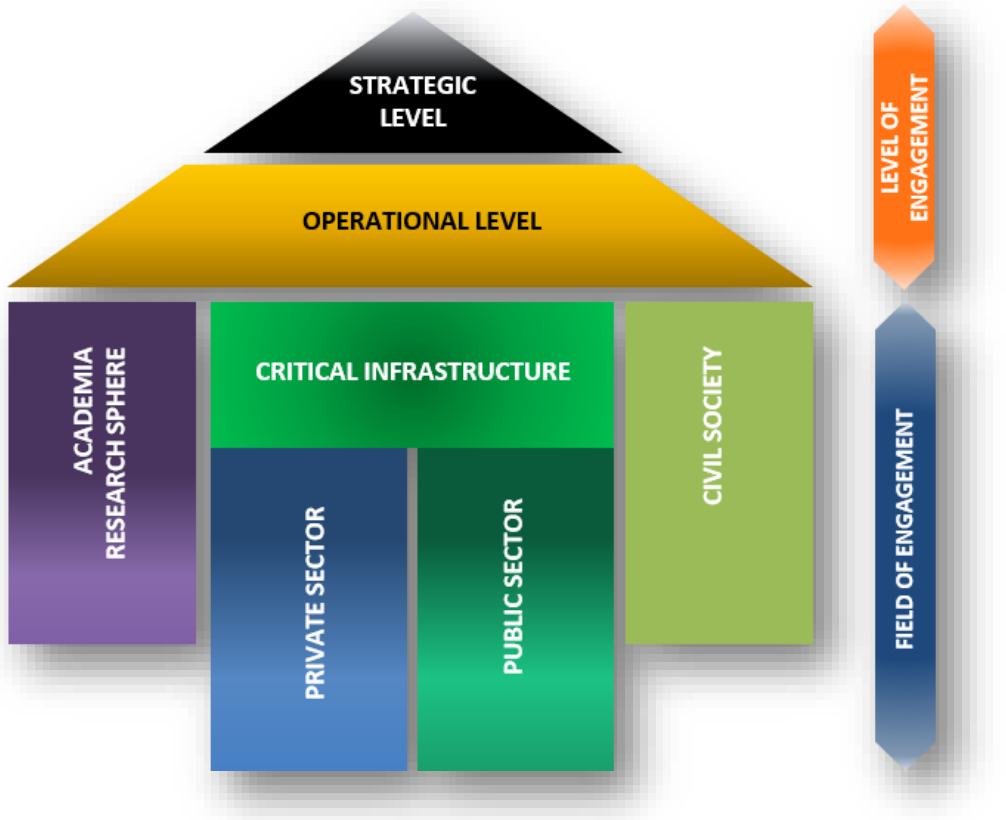

Figure 1: Scheme of the cyber security assurance system

The cyber security assurance system will also include other stakeholders. Operators of critical infrastructure in the private and public sectors are important, particularly in the energy supply sector (electricity producers and distributors), and in information and communication support (telecom operators, information society service providers, etc.).

In awareness raising, education and research, the academic and research community will contribute to the cyber security assurance system through their higher-education programmes and courses on cyber security at all levels of education, and through the results of research organisations. The

system will also be open to civil society's initiatives. This applies primarily to initiatives for improvements and assistance in raising awareness among various target groups by professional associations (Slovenian associations and the Slovenian sections of international associations in the field of information and communication technologies and cyber security).

7 The areas of strategy implementation

Strategy implementation will focus on preventing security incidents, responding to security incidents and increasing awareness of the target groups about the importance of cyber security.

7.1 Prevention

The prevention of security incidents ranges from the technical design of information system components to providing national and international legal frameworks and regulations that contribute to the development of safer applications and infrastructure. Furthermore, it should be ensured that the design of programmes and ICT infrastructure include the safety and protection of individuals' privacy, and that the standards ensuring safe and smooth operation of the systems, including the use of encryption solutions, are observed. Risks are assessed, which serves as a basis for the preparation and implementation of measures to mitigate unacceptable risks, and an analysis of the implemented measures. The use of open-source technologies that ensure interoperability and allow best possible control, and which are not partially of fully closed because of patent rights, is encouraged.

7.2 Response

Prevention alone is insufficient for achieving a high level of cyber security. As security incidents can never be fully eliminated, it is necessary to provide for appropriate mechanisms to respond to them. It is furthermore important to take account of the experience obtained from the prevention phase, as well as from the past security incident response events. Experience may come from domestic and foreign institutions responsible for cyber security assurance, and therefore their best possible interconnectivity is very important. Based on the experience and analysis of incidents and risks, the response measures are constantly updated and improved. Active cooperation is also observed in the preparation of standard cyber crisis response procedures at the international or global level.

7.3 Awareness raising

People are those who develop, build and use ICT. Awareness raising and education may help to eliminate the risks and build a culture of safe technology use. In the awareness-raising phase, the experience derived from prevention and response phases must be utilised so that users are acquainted with actual risks and effective methods of avoiding them. The methods and contents of awareness raising (programmes) are adjusted to various target groups to the greatest possible extent. For children and adolescents, cyber security topics are included in the curriculum at different levels of education. Adjusted awareness-raising programmes for the remaining population and business entities are developed. The use of encryption solutions, as one of the cornerstones of cyber security assurance, is encouraged.

8 Strategy objectives and measures for their achievement

Strategy implementation, which will be based on the upgrade and update of the existing cyber security system capabilities, will be monitored by the Government of the Republic of Slovenia, the central coordination of the national cyber security system, and by the relevant ministries, in accordance with the grounds of jurisdiction set out in the Constitution and legislation.

A number of measures will be carried out to reach the objectives of cyber security. If needed, during the implementation of the strategy, the measures can be upgraded accordingly.

OBJECTIVES	MEASURES
1. Strengthening and systemic regulation of the national cyber security assurance system	• establishing a central coordination of the national cyber security assurance system; • human resource and technological strengthening of bodies at the operative level of cyber security assurance system along with the implementation of SIGOV-CERT; • regular participation in international exercises on cyber security and organisation of national exercises; • gradual upgrade of state bodies' HKOM networks with equipment that is appropriately approved by the Slovenian authorities as being safe and suitable for use; • implementation of competent checks of safety and functionality of IT equipment within the existing and newly established bodies.
2. The safety of citizens in cyberspace;	• regular implementation of awareness-raising programmes on cyber security; • introducing cyber security content in education and training programmes.
3. Cyber security in the economy	• promotion of development and introduction of new technologies in the field of cyber security; • regular implementation of awareness raising programmes on cyber security for business entities.
4. Providing the operation of critical infrastructure in the sector of ICT support	• regular assessment of risks to the operation of the critical infrastructure of the ICT support sector, planning appropriate protection measures and updating risk assessment in this field.
5. Cyber security assurance to ensure public security and combat cyber crime.	• Implementation of appropriate cyber capacities to protect ICT systems of the police; • regular training on cyber security for law enforcement authorities participating in the development of cyber capacities for public security and in combating cyber crime; • regular updating of the laws and procedures in line with the development of ICT.
6. Development of defence cyber capabilities	• development of appropriate cybercapabilities to protect defence ICT systems
7. Ensuring safe operation and availability of	• ensuring conditions for the smooth operation of key ICT

OBJECTIVES	MEASURES
key ICT systems in the event of major natural and other disasters;	systems in the event of major natural and other disasters.
8. Strengthening national cyber security through international cooperation	• ensuring conditions for the participation of Slovenian experts in the relevant international working bodies and associations in the area of cyber security.

Table 1: Cyber security strategy objectives and actions needed to achieve them

8.1 Strengthening and systemic regulation of the national cyber security assurance system

Slovenia will strengthen and upgrade its existing cyber security assurance system, including its diplomatic and consular network. Due to the increasing volume of security incidents, the existing capabilities of the response centres are no longer sufficient. In order to ensure the proper response, the capabilities of the National Response Centre (SI-CERT and the response centre for the needs of the defence and protection against natural and other disaster (cyber capacities of the Ministry of Defence) will be strengthened, and an independent response centre for the public administration systems will be set up (SIGOV-CERT). The framework of strengthening the cyber security assurance system also included the preparation of a plan to respond to security incidents.

At the strategic level of cyber security assurance system, a central coordination for comprehensive approach and coordination of activities in all areas of cyber security will be set up. One of the functions of this coordination will be to act as a single national point of contact for international cooperation in the area of cyber security.

Also in the future, Slovenia will regularly participate in international exercises on cyber security. Besides that, it will also carry out exercises at the national level. The content of each exercise will possibly be consistent with the risk assessment of a specific treat, however, based on the most realistic scenario possible. At least occasionally, exercises will be carried out with the participation of all stakeholder engaged in cyber security assurance. Thus, all the mechanisms, the preparedness and the interaction of participants will be checked. Each exercise will be followed by a detailed analysis of the results and drafting proposals for any improvements and, if necessary, upgrading or updating the security incidents response plan.

To achieve the objective of strengthening and systemic regulation of national cyber security assurance system, the following measures shall be implemented:

- establishing a central coordination of the national cyber security assurance system;
- human resource and technological strengthening of bodies at the operative level of cyber security assurance system along with the implementation of SIGOV-CERT;
- regular participation in international exercises on cyber security and organisation of national exercises;
- gradual upgrade of state bodies' HKOM networks with equipment that is appropriately approved by the Slovenian authorities as being safe and suitable for use;

- implementation of competent checks of safety and functionality of IT equipment within the existing and newly established bodies.

8.2 The safety of citizens in cyberspace

Each individual must be able to have access to the safest possible use of ICT, while respecting privacy and human rights. Citizens must have the opportunity to become acquainted with the risks in cyberspace and means of their control and the associated responsibility of each individual for their own safety in the global communications network. Cyber security assurance should not disproportionately infringe on privacy by using excessive measures or means. All the relevant and interested stakeholders must always be involved in the drafting of the legislation governing permissible degree of intrusion into the privacy of information in a timely and equitable manner.

Raising user awareness about the importance of cyber security is extremely important, as it contributes to building or improving the culture of cyber security. Thus, users learn to independently take care of their own security in cyberspace. Therefore, in addition to further implementation of the existing awareness programmes, new ones will be developed. Participation in various initiatives to raise awareness and involve civil society in these activities will be encouraged. Effective outreach will focus on specific target groups (e.g. children and adolescents, different age groups of citizens, business entities).

Cyber security topics will be properly included in the curricula of schools at all levels of the education system. Furthermore, universities should be encouraged (e.g. by increased demand from the economy) to offer independent study programmes on cyber security. Key stakeholders in cyber security assurance should ensure the development of competences and certification of personnel that perform or will perform the tasks of cyber security assurance by continuous training.

To achieve the objective of ensuring citizens' security in cyberspace, the following two measures will be taken:

- regular implementation of awareness raising programmes on cyber security;
- introducing contents in the area of cyber security in the education and training programmes.

8.3 Cyber security in the economy

As regards ICT in the economy, Slovenia already has a lot of potential, but with adequately focused investments in research, development and innovation, further breakthrough is also possible in the field of cyber security. Cyber security assurance in the economy is particularly important in the digitalised business and industry environment. The state will co-finance projects and targeted research in this field, which have the potential of contributing to cyber security. The applicable results of such projects and research must constantly upgrade the system of cyber security. Likewise in other areas, also in the area of cyber security the state will promote integration of academic and research sphere with the economy at both national and international levels. Thus, it will help to create a critical mass of experts in this field, thereby creating public-private partnerships that will be able to develop innovative products and services with high added value to domestic and global markets.

For its operation, the increasingly digitalised economy should be provided with a secure communication environment. Therefore, programmes to raise companies' awareness about the risks of cyberspace and the secure use of ICT will be continued. In doing so, greater attention will be paid to the identified critical areas in accordance with the current analyses of the situation. Efforts for the development and use of standards in cyber security will be promoted.

To achieve the objective of cyber security in the economy, the following two measures will be taken:

- the promotion of development and introduction of new technologies in the field of cyber security;
- regular implementation of awareness raising programmes on cyber security for business entities.

8.4 Providing the operation of critical infrastructure in the sector of ICT support

Critical infrastructure of ICT support sector must be designed and managed so as to provide systemic ICT support at various levels. The uninterrupted operation of infrastructure must be ensured, which requires the functioning of internet systems, as well as hardware and software that support critical functions in the country. Rapid and efficient mechanisms for responding to threats and debugging, i.e. sanation of damage resulting from security incidents, and preventive mechanisms that as far as possible prevent such threats and errors, are established. By establishing an independent response centre for public administration systems (SIGOV-CERT), SI-CERT will be relieved and thus – with appropriate reinforcement – able to focus attention to providing cyber security in the ICT support sector.

To achieve the objective of ensuring the operation of critical infrastructure in the sector of ICT support, the following measure will be taken:

- regular assessment of risks to the operation of the critical infrastructure of the ICT support sector, planning appropriate protection measures, and updating risk assessment in this field.

8.5 Cyber security assurance to ensure public security and combat cyber crime

Slovenia will develop cyber capabilities that will be able to independently and in cooperation with other countries protect ICT systems in public security (Schengen, Europol, Interpol) and to provide support to operational police work. The development of the capabilities of the police and judicial authorities for combating cybercrime will be accelerated. Greater attention will be paid to the development of digital forensics and care for adequate qualification of all law enforcement authorities operating in this area. Knowledge of cybercrime suppression is also important for successful prosecution of the classic types of crime, as the use of services offered online and other networks is increasing in performing these activities. In the development of cyber capabilities, the state will cooperate with industry and academic institutions. In the detection of new forms of cyber crime and the exchange of information, cooperation of the police with response centres, academic and research institutions, hardware and software producers as well as with professional associations in the field of ICT at national and international level will be important. Legislation and procedures in this area should stay abreast of the rapid development of ICT, and appropriate technical experts should be involved in their drafting.

To achieve the objective of cyber security assurance in the area of public security and combating cyber crime, the following measures will be taken:

- Implementation of appropriate cyber capacities to protect ICT systems of the police;
- regular training on cyber security for law enforcement authorities participating in the development of cyber capacities for public security and in combating cyber crime;
- regular updating of the laws and procedures in line with the development of ICT.

8.6 Development of defensive cyber capabilities

Slovenia will develop cyber defence capabilities that will be able to independently and in cooperation with other EU and NATO countries to protect defence ICT systems and to provide support to military operations and crisis planning. Slovenia will develop its cyber defence capabilities independently as well as in cooperation with its EU and NATO partners, while also cooperating with industry and academic institutions.

To achieve the objective of defence cyber security, the following measure will be taken:

- development of appropriate cyber capabilities to protect defence ICT systems.

8.7 Ensuring safe operation and availability of key ICT systems in the event of major natural and other disasters

Slovenia is exposed to natural and other disasters[15], which may also be large-scale. Therefore, it is necessary to provide adequate resources and implement measures for ensuring the smooth operation of ICT systems in all circumstances, even in the event of major natural and other disasters. Cyber security assurance measures are intended to ensure data integrity as well as the availability, reliability and security of access to services and data.

To achieve the objective of ensuring safe operation and availability of key ICT systems in the event of major natural and other disasters the following measure will be taken:

- ensuring conditions for smooth operation of key ICT systems in the event of major natural and other disasters.

8.8 Strengthening national cyber security through international cooperation

Given the global nature of the Internet and thus also the problems of cyber security, international cooperation in ensuring cyber security for Slovenia as a small country is indispensable. Such cooperation facilitates good exchanges of experience, knowledge and best practices, all of which contribute to the strengthening of national security. Slovenia will therefore continue to promote the participation of its representatives in international organisations such as the UN, EU, NATO, OSCE, OECD and ITU, as well as in international professional associations in this field. It will strive for the

[15] Resolution on the national program for protection against natural and other disasters in the years 2009 to 2015. In: Uradni list RS, 2009, št. 57/2009. Available at: http://www.uradni-list.si/1/objava.jsp?urlid=200957&stevilka=2789.

development of international standards of operation in cyberspace and for the implementation of practical confidence-building measures in cooperation with other countries and international partners. At the international level, Slovenia will take an active part in knowledge transfer in the area of cyber security.

To achieve the objective of national cyber security with international cooperation, the following measure will be taken:

- ensuring conditions for the participation of Slovenian experts in the relevant international cyber security working bodies and associations.

9 Strategy implementation risks

The greatest risk to the strategy's implementation is insufficient awareness about the importance of cyber security assurance, which goes hand in hand with low general security culture, and the lack of political will and consensus for the systemic regulation of this area at the national level. Unsystematic development of such an important area as cyber security assurance would entail very harmful consequences for the state, which would be – in the event of large-scale cyber attacks – difficult to remedy.

Successful implementation of the strategy will, on the contrary, have a positive impact on the assurance of national security, with positive multiplicative effects associated with the increased level of security. It will also have influence on the increase of users' confidence in the Internet and thus the development of new services and business models associated with its use, which will be reflected in digital economic growth and greater social welfare.

STRENGTHS	WEAKNESSES
• Operational level of cyber security assurance has been established. • Quality though insufficient human resources at the operational level of the system. • Good results of the preventive measures (awareness raising programmes) implemented so far. • Participation in common international exercises.	• Strategic level of cyber security assurance has not been established. • Lack of resources (financial, human, material and technical). • Insufficient cooperation between key stakeholders. • The field lacks a regulatory framework.
OPPORTUNITIES	**THREATS**
• Increased trust of users (businesses, state administration, individuals) in the use of the Internet, which increases its use (B2C, B2B, B2G, G2C), lowers operating costs and, consequently, allows digital growth. • The integration of existing capabilities and the utilisation of synergies.	• Insufficient awareness of the importance of the area and the associated lack of political will and consensus for rapid and effective action and systemic regulation at national level. • The possibility of system failure in the event of an increase in security incidents if the system is not reinforced.

Table 2: Analysis of strengths, weaknesses, opportunities and threats to strategy implementation

Being a strategic document, cyber security strategy has no direct financial implications; it is a guiding principle of development activities for cyber security assurance. Financial implications will arise with the implementation of the strategy, which will be limited by the resources available within the respective applicable state budget, thus having regard to Article 23 of the Budget Implementation Act, which provides that the amount earmarked for specific expenditure can only be in the amount specified by the budget. The implementation of the strategy will also be limited by the resources available within the Operational Programme for the Implementation of the EU Cohesion Policy 2014 – 2020.

A List of abbreviations

AKOS	Agency for Communication Networks and Services of the Republic of Slovenia
Arnes	Academic and Research Network of Slovenia
B2B	Business to Business
B2C	Business to Customer
B2G	Business to Government
CERT	Computer Emergency Response Team
ENISA	European Union Agency for Network and Information Security
EU	European Union
G2C	Government to Customer
HKOM	State bodies communication network
ICT	Information and communications technology
IT	Information technology
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
OSCE	Organisation for Security and Cooperation in Europe
SI-CERT	Slovenian National Computer Emergency Response Team
SIGOV-CERT	Public Administration Computer Emergency Response Team
SOVA	Slovenian Intelligence and Security Agency
UN	United Nations