CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Organisation: SLOVENIA

Damjan Štrucl

NATO CCDCOE Strategy Researcher

National Cybersecurity Governance Series

Tallinn 2021

About this study

This publication is part of a series of country reports offering a comprehensive overview of national cybersecurity governance by nation. The aim is to improve awareness of cybersecurity management in the various national settings, support nations enhancing their own cybersecurity governance, encourage the spread of best practice and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO Nations that are Sponsoring Nations of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), each country report outlines the division of cybersecurity roles and responsibilities between agencies, describes their mandate, tasks and competencies and the coordination between them. In particular, it covers the mandates of political and strategic management; operational cybersecurity capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines National Cybersecurity Strategy objectives to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. Since January 2018, CCDCOE has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by the following NATO nations and partners of the Alliance,: Austria, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Reports in this series

National Cybersecurity Organisation in Czechia

National Cybersecurity Organisation in Estonia

National Cybersecurity Organisation in France

National Cybersecurity Organisation in Germany

National Cybersecurity Organisation in Hungary

National Cybersecurity Organisation in Italy

National Cybersecurity Organisation in Lithuania

National Cybersecurity Organisation in Luxembourg

National Cybersecurity Organisation in the Netherlands

National Cybersecurity Organisation in Poland

National Cybersecurity Organisation in Romania

National Cybersecurity Organisation in Slovakia

National Cybersecurity Organisation in Slovenia

National Cybersecurity Organisation in Spain

National Cybersecurity Organisation in Turkey

National Cybersecurity Organisation in the United Kingdom

National Cybersecurity Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation in Israel

Series editor: Kadri Kaska and Keiko Kono.

Information in this document has been checked for accuracy as of May 2021.

Table of Contents

1. Digital society and cybersecurity assessment

Country indicators

2.1 million[1]	Population
1.55 million (76%)[2]	Internet users (% of population)
20.271 thousand[3]	Area (km^2)
25.97 thousand[4]	GDP per capita (USD)

International rankings*

33th[5]	ICT Development Index (ITU 2017)
23th[6]	E-Government Development Index (UN 2020)
17th[7]	Digital Economy and Society Index (EU 2020)
48th[8]	Global Cybersecurity Index (ITU 2018)
40th[9]	National Cyber Security Index (eGA 2020)

1.1 Digital infrastructure availability and take-up

Slovenia has very unfavourable geographical characteristics for fixed broadband connection or mobile 4G broadband coverage: approximately 58 % woods, more than 60 % of mountains and hills, diversity of settlement structure with a large number of small settlements and numerous areas of dispersed settlements. Those small and dispersed settlements represent almost a quarter of all households. Slovenian territory is divided on:

[1] Prebivalstvo, Statistical office, Republic of Slovenia, 2020, https://www.stat.si/StatWeb/, accessed on 2. 12. 2020.
[2] Digitalna družba, Statistical office, Republic of Slovenia, 2020a, (Proportion of people aged 16 to 74 who use the Internet every day or almost every day, regardless of place (at home, at work, school, etc.) or purpose of use (private, business)), https://www.stat.si/StatWeb/Field/Index/25, accessed on 2. 12. 2020.
[3] Statistical office, Republic of Slovenia, 2018, p. 1, https://www.stat.si/StatWeb/File/DocSysFile/10033/Spremembe_povrsine_Slovenije.pdf
[4] BDP in nacionalni računi, Statistical office, Republic of Slovenia, 2020b, Republic of Slovenia, 2020, https://www.stat.si/StatWeb/Field/Index/1, accessed on 2. 12. 2020.
[5] ICT Development Index 2017, International Telecommunication Union, 2017, https://www.itu.int/net4/ITU-D/idi/2017/index.html, accessed on 2. 12. 2020.
[6] E-Government Survey 2020, Digital Government in the Decade of Action for Sustainable Development, United Nations, 2020, p. 51, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020 UN E-Government Survey (Full Report).pdf
[7] European Union, Digital Economy and Society Index 2020, 2020, p. 14, https://eufordigital.eu/wp-content/uploads/2020/06/DESI2020Thematicchapters-FullEuropeanAnalysis.pdf
[8] Global Cybersecurity Index (GCI) 2018, International Telecommunication Union, 2018, p. 61, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[9] National Cyber Security Index (NCSI), Slovenia, e-Governance Academy, 2020, https://ncsi.ega.ee/country/si/, accessed on 2. 12. 2020.

- Urban areas (163 settlements or 3 % of all settlements) cover 4 % of Slovenia's territorial area. In those urban areas live 45 % of population and the average air distance from the subscriber to the active devices that enable broadband connection is 0.7 km.
- Suburban areas (1453 or 24 % of all settlements) cover 16 % of Slovenia's territorial area. In those suburban areas live 31 % of population and the average air distance from the subscriber to the active devices that enable broadband connection is 1.2 km.
- The remaining rural areas (44200 settlements or 73 % of all settlements) cover 80 % of Slovenia's territorial area. In those rural areas live 24 % of population and the average air distance from the subscriber to the active devices that enable broadband connection is 2.2 km.[10]

In line with the European Digital Agenda 2020, in 2016 the Digital Slovenia Strategy (DSS 2020) has been adopted and was updated with the plan for the introduction of next generation networks in 2018. According to the DSI 2020, Slovenian plan has been providing broadband internet access speed of at least 100 Mbps to 96 % of households and at least 30 Mbps of the internet speed for remaining 4 % of households by 2020. However, these goals have not been achieved yet.[11]

Despite those facts, 90 % of Slovenian are connected to the internet[12] with the proportion: 34.7 % over 100 Mbps of speed (ultrafast broadband), 25.7 % between 30 up to 100 Mbps of speed, 31. 5 % between 10 up to 30 Mbps of speed, 7.5 % between 2 up to 10 Mbps of speed, and 0.5 % less than 2 Mbps of speed. Fixed broadband internet penetration by households continues the growth trend and increased by 0.5% compared to the previous quarter, reaching 83.7% in the first quarter of 2020.[13]

Despite unfavourable geographical characteristics, Mobile 4G/LTE broadband coverage of the landscape of Slovenia is 96 % and 86 %[14] of companies use mobile broadband internet access.[15]

Slovenia does not have a developed 5G network yet. However, it has a commercial 5G network, which has been established by Telekom Slovenije in July 2020.[16] According to the Slovenian National Broadband Plan 2025, Slovenia is planning to make 5G network coverage in urban areas and the main terrestrial transport routes by 2025.[17] In September 2020 Slovenian Government adopted a decision on measures for ensuring cyber security in 5G networks which provides the basis for the implementation of the 5G Toolbox in legislation from the field of electronic communications.[18]

According to the Digital Economy and Society Index (DESI) 2020 of the EU, Slovenia achieved a great improvement of the DESI evolution over the time. The data shows that Slovenian DESI evolution has

[10] Next-Generation Broadband Network Development Plan to 2020, Republic of Slovenia, 2016, pp. 8-9, https://www.gov.si/assets/ministrstva/MJU/DID/NGN_2020_Slovenia_EN.pdf
[11] Ibid, pp. 2-4.
[12] Digitalna družba, Statistical office, Republic of Slovenia, 2020a, https://www.stat.si/StatWeb/Field/Index/25, accessed on 2. 12. 2020.
[13] Poročilo o razvoju trga elektronskih komunikacij za prvo četrtletje 2020, The Agency for Communication Networks and Services of the Republic of Slovenia, 2020, p. 13, https://www.akos-rs.si/fileadmin/user_upload/Cetrtletno_porocilo_Q1_2020_za_objavo.pdf
[14] Digitalna družba, Statistical office, Republic of Slovenia, 2020a, (Proportion of companies with 10 or more employees with mobile broadband internet access (at least 3G modem or 3G mobile phone)), https://www.stat.si/StatWeb/Field/Index/25, accessed on 2. 12. 2020.
[15] Sloji pokritosti, Geoportal AKOS, 2020, https://gis.akos-rs.si/HomePublic/OPTPogledResult/slo
[16] Telekom Slovenije, Prvo 5G omrežje Slovenije, 2020, https://www.telekom.si/5g, accessed on 2. 12. 2020.
[17] EU, Digital Economy and Society Index (DESI) 2020 Slovenia, 2020a, p. 5, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929
[18] Novice, Republika Slovenija, 2020, https://www.gov.si/novice/2020-09-29-98-dopisna-seja-vlade-republike-slovenije/, accessed on 2. 12. 2020.

been steadily growing since 2015. Slovenia ranks 16th out of 28 EU Members States but still continues to lag behind the EU average since EU is ranked 14th.[19]

1.2 Digital public services

The Government of Republic of Slovenia has adopted four main strategic documents relating to the information society and to the Digital Single Market of EU respectively:

- Public Administration Development Strategy 2015 – 2020[20],
- DSI 2020,
- Next-Generation Broadband Network Development Plan to 2020[21],
- And National Cyber Security Strategy (NCSS)[22].

By these strategies, the Government of the Republic of Slovenia sets objectives to bolster the efficiency and security of digital public services provision. Through its strategic goals it strives to develop public-private partnership, high speed open internet for all residents, quality digital public administration, the effective and safe usage of the digital public services, trust and confidence in cyber space, secure cyberspace and protection of human rights, and raise awareness of the importance of ICT and cyber threats.[23]

Digital Slovenia 2020 together with the Slovenian Industrial Policy (RISS – Research and Innovation Strategy of Slovenia and SIP - Slovenian Industry Policy) covers all areas of life and development of digital environment: entrepreneurship, public services, households and education. Currently, three strategies are under development or update: All-inclusive artificial intelligence strategy, Data strategy and the Digital Slovenia strategy respectively.[24]

E-governance

E-governance in Slovenia is run and implemented by Ministry of Public Administration based on Article 34.a of the Civil Service Law[25]. Within Ministry of the Public Administration the Information Society and Informatics Directorate is responsible for the strategic planning, promoting the digital transformation of Slovenia, the functioning of the national communication network, and is acting as the Single Contact Centre for all governmental institutions. The Directorate represents the Republic of Slovenia (RS) in international organisations and is responsible for the issuing of the digital certificates, developing the

[19] EU, Digital Economy and Society Index (DESI) 2020 Slovenia, 2020a, p. 3, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929

[20] Public Administration Development Strategy 2015 – 2020, Republic of Slovenia, 2015, https://nio.gov.si/nio/asset/strategija+razvoja+javne+uprave+2015+2020?lang=en

[21] Next-Generation Broadband Network Development Plan to 2020, Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/NGN_2020_Slovenia_EN.pdf

[22] Cyber Security Strategy, Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf

[23] Digital Transformation of Slovenia, Republic of Slovenia, 2017, http://www.tirana.embassy.si/fileadmin/user_upload/dkp_55_vti/docs/Digital_transformation_of_Slovenia.pdf

[24] EU, Digital Economy and Society Index (DESI) 2020 Slovenia, 2020a, p. 3, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929

[25] Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14 in 51/16 (available only in Slovenian), Zakon o državni upravi (ZDU-1), neuradno prečiščeno besedilo 18, 2016, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3225

public cloud, e-services, Digital Single Market, data management, the implementation of the unified IT security policy act.[26]

The structure of the Information Society and Informatics Directorate is based on its responsibilities. Its composition is as follows: Infrastructure Office, User Support Office, Digital Solutions Development Office, Information Society Office, Information Security Division, Strategic Development and Competence Division, Business Economics Division, Trust Service Division, and System architecture and Hosting Operations Management Division. Information Society and Informatics Directorate also hosts SIGOV-CERT, the State Administration Bodies Computer Emergency Response Team, which is not the same as the national CERT (see Section 3.2).[27]

The Ministry of Public Administration does not straightforward follow ISO or NIST standards, but rather has set its own standards by partially implementing ISO standards into one role book and two methodologies: Rules on security documentation and security measures of state administration bodies,[28] Methodology of information security risk management in public administration, and Unified methodology for inventory of information assets and information systems in state administration. By this role book and methodologies minimal sets of standards have been established regarding the information security of government IT and providers of essential services: Information security risk management, Information security management, Business continuity management system and Inventory of information assets and own information systems.[29]

The area of digital public services is covered by several different national laws and regulations, and EU regulation[30] as well. The underlying binding law is Electronic Communications Act[31] which must be abided by all providers of electronic communications network and electronic communications services (Article 4). In accordance with the provisions of this Act, a vast number of the Decree and Rules have been adopted, which regulate the field of electronic communications network and electronic communications services in

[26] Information Society and Informatics Directorate, 2020, https://www.gov.si/en/state-authorities/ministries/ministry-of-public-administration/about-the-ministry/information-society-and-informatics-directorate/, accessed on 2. 12. 2020.
[27] Ibid.
[28] Uradni list RS, št. 68/19 (available only in Slovenian), Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave, 2019, http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV13669
[29] Informacijska varnost, Republika Slovenija, 2020, https://www.gov.si/teme/informacijska-varnost/, accessed on 2. 12. 2020.
[30] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, Official Journal of the EU, L 321/36; Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the EU, L 194/1, Directive 2009/136/EC of the European Parliament and of the Council of 25 November amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the EU, L 337/11; Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, Official Journal of the EU, L 337/37.
[31] The new Electronic Communications Act will be adopted at the end of 2020 or at the beginning of 2021. (Republika Slovenija, Zakon o elektronskih komunikacijah (available only in Slovenian), 2020, https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10097, accessed on 2. 12. 2020; Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17, Zakon o elektronskih komunikacijah (ZEKom-1), NPB št. 5 , 2017, http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405; Official Gazette RS, no 109/12, 110/13, 40/14 - ZIN-B, and 54/14 - Decision of the Constitutional Court no. U-I-65/13, Electronic Communications Act, 2013, https://www.legislationline.org/download/id/5561/file/Slovenia_Electronic%20Communications%20Act_2014_en.pdf)

Slovenia in more detail. In addition to this law, there are several other acts, such as Electronic Commerce and Electronic Signature Act, Act on Conditional Access to Protected Electronic Services, Law on Digital Broadcasting, Information Security Act, and Decree on information security in state administration. All these laws, together with EU rules, form a common legal framework for the provision of digital public services.[32]

Digital public services

In 2001 the first eGovernment portal e-Uprava was lunched and has been modernised several times since then.[33] A vast number of public services have been established since then: insights into own personal data and public/ own real estate data, social services, labour services, e-taxes, e-health, digital signatures and digital ID, etc. In addition, Slovenia established business portals for domestic and foreign entrepreneurs (e-VEM and EUGO) and integrated both into the national business point (Slovenska poslovna točka – SPOT).[34] However, only 59% of internet users are active in e-government, which represents 8% below an EU average (67%). Almost the same situation is seen regarding the digital public services for businesses where Slovenia with 77% lagging behind an EU average of 88%. Nevertheless, Slovenia has better scores on pre-filed forms (64%), online service completion (91%) and open data (75%) compared to an EU average 59%, 90% and 66%, respectively. To support digital public services the Single Contact Centre has been established. All citizens and public employees can get user support through telephone, e-mail or online forms.[35] Thus, in digital public services Slovenia is ranked 17th and in the open data 10th among EU countries. Therefore, Slovenia's further plan is to roll out a national e-identity card in 2021, thereby increasing the use of e-services.[36]

The Ministry of Public Administration is also responsible for the Slovenia State Cloud (Državni računalniški oblak – DRO[37]). The purpose of the DRO is to ensure service connectivity, establish a single service platform based on a common architecture for improving the accessibility of public services to citizens, and ensure the availability of services from anywhere and anytime and to provide effective information security. Regarding DRO, the Ministry of Public Administration in 2015 has received an award from the American company EMC for the most innovative IT project in Central Europe with a reference solution that no other country in the region had before, and in 2018 also obtained the ISO/IEC 27001:2013 certificate.[38]

---

[32] Zakonodaja Ministrstva za javno upravo, Republika Slovenija, 2020, https://www.gov.si/drzavni-organi/ministrstva/ministrstvo-za-javno-upravo/zakonodaja/, accessed on 2. 12. 2020.

[33] eGovernment in Slovenia, European Commission, 2015, p. 18, https://joinup.ec.europa.eu/sites/default/files/inline-files/eGov%20in%20Slovenia%20-%20January%202015%20-%20v_18_0_Final.pdf

[34] Those services are: running the business, taxation, selling in EU, financing and funding, product requirements, human resources, and dealing with customers. (Digital Government Factsheet 2019 Slovenia, EU, 2019, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf

[35] Information technology in public administration, Republic of Slovenia, 2020, https://www.gov.si/en/topics/informatika-v-drzavni-upravi/, accessed on 2. 12. 2020.

[36] EU, Digital Economy and Society Index (DESI) 2020 Slovenia, 2020a, pp. 12-13, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929; OECD, Digital Government Review of Slovenia Leading the digitalisation of the public sector, 2020, https://www.oecd.org/gov/digital-government/digital-government-review-slovenia-highlights.pdf; European Union, Digital Government Factsheet 2019 Slovenia, 2019, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf

[37] Državni računalniški oblak: https://nio.gov.si/nio/asset/drzavni+racunalniski+oblak+dro?, accessed on 2. 12. 2020.

[38] Information technology in public administration, Republic of Slovenia, 2020, https://www.gov.si/en/topics/informatika-v-drzavni-upravi/, accessed on 2. 12. 2020.

1.3 Digitalisation in business

Slovenia has been promoting digitalisation of the private sector and industry since 2017, when the Chamber of Commerce has established the Digital Academy. Slovenia is aware of human capital who is essential for digitalisation of the whole society, therefore the commercial sector runs Digital Coalition to bolster goals and objectives of Slovenian digital transformation drawn in Digital Slovenia 2020, the Research and Innovation Strategy of Slovenia, as well as the Smart Specialization Strategy. The outcome of all those strategies are establishment of the Strategic Research and Innovation Partnerships (SRIPs)[39], the Digital Innovation Hubs (DIH), and the FabLabs[40]. In addition, Slovenia developed the comprehensive programme of digitisation and digital transformation of Small and Medium-Sized Enterprises (SMEs) 2018-2023.[41]

According to the DESI for Slovenia, 81% of Slovenian population use the internet (EU 85%), of which 66% internet users shopping and 22% selling online (the EU averages are 71% and 23%, respectively). The lagging behind EU is on the field of banking (57% of internet users) and SMEs selling online (17%), where the EU average is 66% and 18%, respectively. Despite lower percentage on those fields, Slovenia has a better average than EU (8%) on the cross-border sell online (12%) and the same average as EU regarding e-commerce turnover (11%). In terms of the integration of digital technology by businesses, Slovenia has lost one place in ranking and it has been ranked 15th among EU countries in 2019. According to the European Investment Bank, 75% of Slovenian firms have implemented at least one digital technology that represents about 18% above the average of EU (57%). The best digital developed sectors are e-commerce, automotive, tourism, robotics, fin-tech, artificial intelligence, cyber security, innovation of composite materials, and companies integrated into foreign value, yet, still is lagging behind in integration of digital technology into the business processes.[42]

1.4 Cyber threat landscape and cybersecurity assessment

The NCSS, adopted in 2016, does not directly address cyber threats, but rather addresses threat actor agnostic and cyberspace risks. Extremely rapid development of ICT, Internet dependency, cybercrime, intelligence activities and changes of the security environment have been identified as the biggest cyberspace risks. Nevertheless, cyber-attacks can be indirectly identified as a cyber-threat, as the strategy recognized them as the most significant threats to the modern world as a whole and insufficient cyber security awareness regarding them as well. With both threats are associated lack of the political will and consensus regarding systemic regulation at national level.[43]

In 2018, the Ministry of Public Administration published the Cyber threats assessments[44]. This document has been prepared in accordance with the Decree on Implementation of the Decision of the EU

[39] Strategic Development and Innovation Partnerships (SRIP) are long-term partnerships between the business community, research organizations, the state and municipalities, and the promotion of partners, innovation users and non-governmental organizations. (European Union, Digital Economy and Society Index (DESI) 2020 Slovenia, 2020a, p. 11, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929)

[40] FabLab is the national reference network of creative laboratories. The main goal of this network is to discover and use the entrepreneurial potential of local communities in Slovenia. There are a total of 28 FabLab laboratories in Slovenia. (Ibid.)

[41] EU, Digital Economy and Society Index (DESI) 2020 Slovenia, 2020a, p. 4, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929

[42] Ibid.

[43] Cyber Security Strategy, Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf

[44] Ocena kibernetskih tveganj (only in Slovenian) Republika Slovenija, Ministrstvo za javno upravo, 2018, https://www.gov.si/assets/ministrstva/MJU/DI/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf

mechanism in the Field of Civil Protection.[45] It is a very comprehensive document, as it classifies cyber threats and addresses the actors of cyber threats, cyber-attack vectors, cyber security in the RS, cyber risk scenarios, risk analysis and risk impact assessment in the line with the NCSS. The document classifies 16 cyber threats and eight cyber threat actors. The cyber threat classification has been made according to the classification of the European Cybersecurity Agency (ENISA) as follows: Malware, Web Based Attacks, Web Application Attacks, Phishing, Spam, Denial of Service, Ransomware, Botnets, Insider treats, Physical manipulation/damage/theft/loss, Data Breach, Identity Theft, Information leakage, Exploit Kits, Cyber Espionage and Hybrid threats. It also has noted that Hybrid threats are not cyber threats per se, but they are very often a part of them and vice versa. Regarding the main cyber threat actors the following actors have been identified: The Cyber criminals, Insiders, States, Hacktivists, Cyber warriors, Cyber terrorists, and Script kiddies. Based on the classified cyber threats, cyber threat actors, and cyber-attack vectors, three different scenarios were developed: 1. Attack with extortion program 2. Attack on state administration web sites, 3. Attack on critical infrastructure in the energy sector and they have been ranked from the most likely to the less likely, respectively.[46]

2. National cybersecurity strategy and legal framework

2.1 National cybersecurity foundation

Slovenia's current NCSS was drafted through interministerial coordination/consultation and in cooperation with the Agency for Communication Networks and Services of the Republic of Slovenia (AKOS), Energy Agency of the Republic of Slovenia, National Security Council (NCS), Office of the Government of the Republic of Slovenia for the Protection of Classified Information, national CSIRT, and Slovenian Intelligence and Security Agency.[47] The NCSS was adopted by the Government in February 2016, without the Cyber security strategy implementation plan, which is the biggest drawback.[48] In June 2020, a new EU Cyber Security Strategy was adopted, so Slovenia plans to renovate the NCSS and DSI 2020, since the DSI was valid to the end of 2020 and the new one is planned to be valid until 2027.[49]

The NCSS was followed by the DSI, which was also prepared in interministerial coordination/consultation. The DSI has been adopted by the Government in March 2016. Among other strategic objectives, a comprehensive cyber security system was set as strategic objective as well. To achieve this objective, the government has envisaged measures such as the establishment of a central coordination unit, the

[45] Uradni list RS, št. 62/14 in 13/17 (available only in Slovenian), Uredba o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite, NPB št. 1, 2017, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED6795. The RS transposed Article 6 (a, b, c) of the Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924) into the Decree on Implementation of the Decision of the EU mechanism in the Field of Civil protection. Ibid.

[46] Ocena kibernetskih tveganj (only in Slovenian) Republika Slovenija, Ministrstvo za javno upravo, 2018, pp. 6-23, https://www.gov.si/assets/ministrstva/MJU/DI/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf

[47] Cyber Security Strategy, Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf

[48] National Cyber Security Index (NCSI), Slovenia, e-Governance Academy, 2020, https://ncsi.ega.ee/country/si/, accessed on 2. 12. 2020.

[49] Strategija kibernetske varnosti: učinkovit sistem zagotavljanja kibernetske varnosti ni zastonj, Republika Slovenija, 2020, https://www.gov.si/novice/2020-08-05-strategija-kibernetske-varnosti-ucinkovit-sistem-zagotavljanja-kibernetske-varnosti-ni-zastonj/, accessed on 2. 12. 2020.

establishment of a governmental CERT (SIGOV-CERT), regular critical infrastructure risk assessment, etc., for which it has planned EUR 4.0 million for the 2016-2020 period.[50]

In accordance with Directive (EU) 2016/1148 (NIS Directive), the Ministry of Public Administration, in cooperation with other ministries, prepared the Information Security Act, which was adopted by the government in 2018. It is a main legal act to regulate the provision of cyber defence and provide preservation essential services of key social and economic activities in the RS.[51]

In addition, the Decree on Information Security in the State Administration was adopted in the same year, which sets minimum common requirements regarding information security in the state administration and which entities shall be established in the state administration authorities.[52]

2.2 National cybersecurity strategy

The NCSS includes an overview of the situation in those areas that are important for ensuring cyber security, and describes the vision and sets objectives. The vision and the objective of the NCSS is establishment of the comprehensive system for ensuring cyber security as an integral part of national security and thus ensuring an open, safe and secure cyberspace for state authorities, the economy and the individual. Therefore, the comprehensive cyber security assurance system is planned to be pyramided, from strategic level to the technical level (Figure 1).[53]

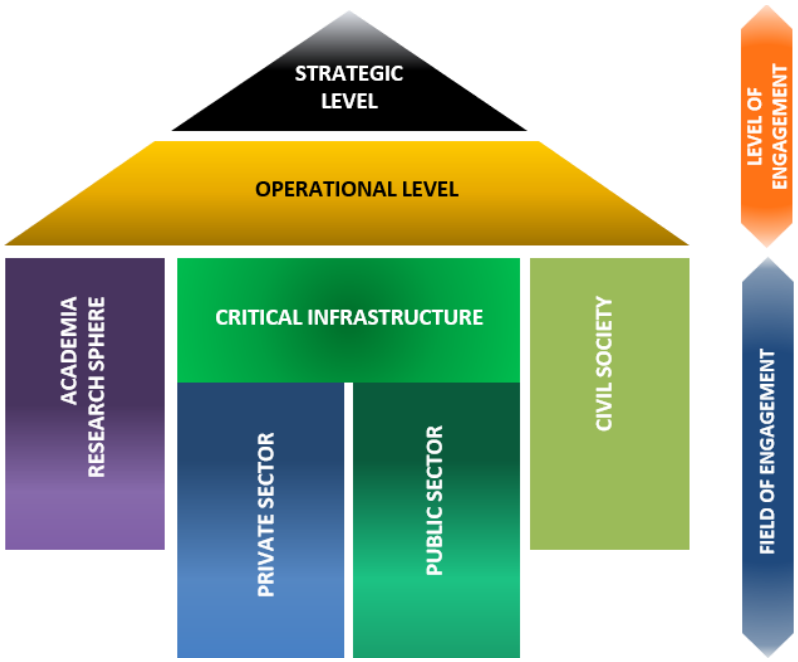


Figure 1: Slovenian information (cyber) security architecture[54]

[50] Digital Slovenia 2020 – Development Strategy for the Information Society until 2020, Republic of Slovenia, 2016, pp. 38-39, https://www.gov.si/assets/ministrstva/MJU/DID/Digital-Slovenia-2020-Development-Strategy-for-the-Information-Society-until-2020.pdf

[51] Uradni list RS, št. 30/18, Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

[52] Uradni list RS, št. 29/18 in 131/20 – NPB št. 1 (available only in Slovenian), Uredba o informacijski varnosti v državni upravi, 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7198

[53] Cyber Security Strategy, Republic of Slovenia, 2016, pp. 2-6, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf

[54] Ibid, p. 9

At the strategic level Slovenia recognizes the need for a central coordination of the national cyber security assurance system, which will be responsible for the implementation of NCSS, coordination of the cyber security assurance capabilities at the strategic level, and will represent a single point of contact at the international level.

Slovenia's national cyber security capabilities and their roles are defined at the operational level: SI-CERT will be the national asset of cyber security assurance, the MORS will be responsible in the field of defence and protection against natural and other disasters (including the protection of critical infrastructure), the police will ensure cyber security in the context of public safety and the fight against cyber crime, Slovenian Intelligence and Security Agency (SOVA) will conduct counter intelligence, and the emergent SIGOV-CERT will be responsible for cyber security in public administration. At the field of engagement other stakeholders also will be included, such as the operators of critical infrastructure in the private and public sectors. To this end, eight sub-objectives and measures have been set by 2020, however, without an Action plan defined:

1. **Strengthening and systemic regulation of the national cyber security assurance system, including its diplomatic and consular network** to enhance national and international cyber security through forming national cyber security system, upgrading ICS, human resource management, and international cooperation.
2. **Enhancing citizen security in cyberspace, including respecting privacy and human rights** by implementation of regular awareness-raising programmes on cyber security and introducing cyber security content in education and training programmes at all levels of the education system.
3. **Promoting cyber security in the economy,** by comprehensive approach through public-private partnership, integration of academic and research sphere, and developing and using standards in the cyber security domain.
4. **Ensuring the functioning of critical infrastructure in the sector of ICT support with responding and preventing mechanisms in place**, by implementing effective risk management of critical infrastructure (regular risk assessment, planning appropriate protection measures).
5. **Enhancing cyber security assurance to ensure public security and combat cyber crime**, by regular updates of the laws and procedures, proper human resource management, regular trainings on cyber security, and the cooperation with industry, academia and the international community.
6. **Development of appropriate defence cyber capabilities**, independently and in cooperation with EU, NATO, industry and academia, to protect defence ICT systems.
7. **Ensuring safe operation and availability of key ICT systems in the event of major natural and other disasters** by providing adequate resources and implementing adequate measures, to ensure conditions for the smooth operation of key ICT.
8. **Strengthening national cyber security through international cooperation** by striving for the development of international standards of operation in cyberspace and for the implementation of practical confidence-building measures, to ensure conditions for the international participation of Slovenian experts in the area of cyber security. [55]

2.3 Cybersecurity legislation

Regarding cyber security, the RS has adopted several different laws that are directly or indirectly related to the protection of information environment and cyberspace, respectively.

Network and information systems security

The cornerstone of Slovenian cyber security legislative framework is the ZInfV. It has come into force on 11 May 2018 and has been complemented by a set of implementing regulations:

[55] Cyber Security Strategy, Republic of Slovenia, 2016, pp. 8-16, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf

- Decree on Information Security in the State Administration,[56]
- Regulation on the definition of essential services and a more detailed methodology for determining the providers of essential services,[57]
- Rules on security documentation and security measures for providers of essential services,[58]
- Methodology of information security risk management in public administration,[59]
- Unified methodology for inventory of information assets and information systems in state administration.[60]

Article 1 of the ZInfV regulates measures on the security of network and information systems in the RS, which are essential for the smooth functioning of the state in all security conditions and provide essential services for maintaining key social and economic activities in the RS. It lays down minimum security requirements and incident reporting requirements for those liable to this Act. It also regulates the responsibilities, tasks, organisation and operation of the competent national information security authority, the single contact point for information security, the national electronic network and information security incident handling teams (national CSIRTs), and electronic network security incident resolution teams and information of state administration bodies (CSIRT of state administration bodies) in the field of information security.[61]

The imposed legal obligation (security requirements, security documentation, security measures, notification of incident, and jurisdiction and territoriality) of the subjects liable under the ZInfV are addressed in Chapter III (Essential services providers), IV (Digital services providers), and V (Public administration). Additionally, no standards are set up in the ZInfV, but subjects are encouraged to use European or internationally accepted standards and specifications (Article 19).[62]

Supervision over the implementation of the provisions of this Act is set out in Chapter X of the ZInfV, and is performed by information security inspectors of the competent national authority (Information Security Administration - ISA), who also cooperates with the Information Commissioner.[63]

Cybersecurity of critical infrastructure

The Information Security Act (ZInfV) does not addresses critical infrastructure protection as such, but determines the essential service providers (Article 5 of the ZInfV: energy, digital infrastructure, drinking water supply and distribution, food supply, healthcare, transport, banking, financial market infrastructure and environmental protection) that coincide with the critical infrastructure sectors defined in the Critical

[56] Uradni list RS, št. 29/18 in 131/20 – NPB št. 1 (available only in Slovenian), Zakon Uredba o informacijski varnosti v državni upravi, 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7198
[57] Uradni list RS, št. 39/19 (available only in Slovenian), Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev, 2019, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7808
[58] Uradni list RS, št. 32/19 (available only in Slovenian), Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev, 2019, http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV13624
[59] Ministrstvo za javno upravo, Republika Slovenija, Metodologija obvladovanja tveganj informacijske varnosti v državni upravi (available only in Slovenian), 2019, https://www.gov.si/assets/ministrstva/MJU/DI/Informacijska-varnost/Metodologija-obvladovanja-tveganj-informacijske-varnosti-v-drzavni-upravi.pdf
[60] Ministrstvo za javno upravo, Republika Slovenija, Enotna metodologija popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi (available only in Slovenian), 2019, https://www.gov.si/assets/ministrstva/MJU/DI/Enotna_metodologija_popisovanja_inf_premozenja_in_sistemov_v_DU.pdf
[61] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707
[62] Ibid.
[63] Ibid.

Infrastructure Act (ZKI).[64] The ZKI and the related implementing regulatory provisions were drafted by the MORS and adopted by the Government of the Republic of Slovenia in 2018 and 2019. While the ZInfV stipulates measures for the high security of networks and information systems, the ZKI stipulates general safety, defines critical infrastructure sectors and determines the responsibilities of critical infrastructure holders (responsible ministries according to a specific critical sector) and operators.[65]

The ZKI does not directly address information / cyber security, but governs the identification and designation of the critical infrastructure of the RS, the principles and planning of the critical infrastructure protection, the duties of the bodies and organizations in the critical infrastructure field, the notification, reporting, and provision of support in the decision-making process, the data protection, and the supervision in the critical infrastructure field.[66] Therefore, it is also necessary to take into account Article 5 of the ZInfV, which coincides with Article 4 of the ZKI (critical infrastructure sectors) and supplements it with additional subjects, as follows:

- Essential service providers (energy sector, information and communication networks and systems sector, drinking water supply and distribution, food supply, health care sector, traffic sector, financial market infrastructure, banking sector, and environmental protection) are stipulated by government,
- Digital services providers,
- State administration bodies that manage information systems and parts of the network or provide information services necessary for the smooth operation of the state or for ensuring national security.[67]

Article 5 of the ZKI stipulates that the criteria for the identification of critical infrastructure are developed on the basis of the estimation of possible consequences of serious disturbances in the operation of the critical infrastructure or its interruption for the national security, economy and other vital societal functions, and health, safety, protection, and the social well-being of people. The criteria for the identification of critical infrastructure serve as a basis for the designation of critical infrastructure and are detailed by the Government. The criteria for the identification of the critical infrastructure are sectoral and cross-cutting criteria, however, the MORS is designated as the holder for implementation of critical infrastructure protection (Article 13 of ZKI).[68]

Therefore, the critical infrastructure operators of the RS are also operators of essential services under the ZInfV and as such are obliged to prepare security documentation and plan security measures as determined by the Rules on security documentation and security measures of operators of essential services (Official Gazette of the RS, No. 32/19). Those measures are part of critical infrastructure protection measures.[69]

The ZInfV in Article 7 also identifies the threasholds/ criteria to be considered in determining the impact, such as for example the number of users affected by the disruption in the provision of the essential service, duration of the incident, geographical distribution as regards the area afected by the incident.[70]

---

[64] Uradni list RS, št. 30/18, Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

[65] Uradni list RS, št. 75/17 (available only in Slovenian), Zakon o kritični infrastrukturi (ZKI), 2017, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7106#

[66] Uradni list RS, 75/17 (available only in Slovenian), Zakon o kritični infrastrukturi (ZKI), 2017, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7106#

[67] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

[68] Uradni list RS, 75/17 (available only in Slovenian), Zakon o kritični infrastrukturi (ZKI), 2017, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7106#

[69] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

[70] Ibid.

Regulations in the field of electronic communications and electronic commerce

In the field of electronic communications and electronic commerce, the RS has adopted three primary legal acts that regulate the function and usage of electronic communications and determine the responsibilities and duties of users and providers of digital services:

- Electronic Communications Act[71] - Regulates the conditions for the provision of electronic communications networks and communication services, radio spectrum management, provision of competition and universal services, restriction of property rights, determines user's rights, regulates network and service security and their operating in emergency conditions, regulates security, privacy of users of public communications services, regulates the competence, organization and operation of the AKOS and certain other issues related to electronic communications;
- Electronic Commerce and Electronic Signature Act[72] - Stipulating the obligations of digital service operators regarding network security, storage of traffic data, prevention of unwanted communications, processing of personal data and protection of privacy of electronic communications;
- Electronic Commerce Market Act[73] - Identifying the responsibilities of digital service providers relating data protection when a digital environment is used for commerce.[74]

Although these laws do not explicitly contain the term information or cyber security, they nevertheless impose obligations on digital service providers regarding the security of cyberspace operations.

Cyber defense

The subjects of cyber defence of the Republic of Slovenia are stipulated in Article 24 of the ZInfV. The national cyber defence is coordinated and implemented by the competent national authority, national CSIRT, the CSIRT of state administration bodies, MORS, police, SOVA and other national authorities in accordance with their competencies in providing national security. Their tasks and responsibilities are to provide adequate cyber defence capabilities in cyberspace, permanently monitor the situation and respond to events in cyberspace. In addition, for the purpose of cyber defence, these entities shall implement coordinated organisational, logical-technical, technical and administrative measures and activities at various levels to ensure comprehensive information security in accordance with their

[71] Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17, Zakon o elektronskih komunikacijah (ZEKom-1) (available only in Slovenian), NPB št. 5, 2017, http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405; Official Gazette RS, no 109/12, 110/13, 40/14 - ZIN-B, and 54/14 - Decision of the Constitutional Court no. U-I-65/13, Electronic Communications Act, 2013, https://www.legislationline.org/download/id/5561/file/Slovenia_Electronic%20Communications%20Act_2014_en.pdf. (The new Electronic Communications Act will be adopted at the end of 2020 or at the beginning of 2021. Predlog predpisa, Zakon o elektronskih komunikacijah, 2020, https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10097, accessed on 2. 12. 2020.)

[72] Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14 (available only in Slovenian), Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), NPB št. 6, 2014, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1973; Official Gazette RS, no 57/2000 - Official Consolidated Text and 25/2004) Electronic Commerce and Electronic Signature Act, 2004, http://cyberlawsconsultingcentre.com/wp-content/uploads/2electronic-commerce-and-electronic-signature-act-2000.pdf

[73] Official Gazette RS, no 96/09 - Official Consolidated Text and 19/15) Electronic Commerce Market Act, Unofficial consolidated version No. 4, 2015, http://www.pisrs.si/Pis.web/npbDocPdf?idPredpisa=ZAKO6919&idPredpisaChng=ZAKO4600&type=doc&lang=EN

[74] Štrucl, D., Pravni in institucionalni vidiki ureditve kibernetske varnosti in obrambe Republike Slovenije, 2020, pp. 147-151, https://revis.openscience.si/IzpisGradiva.php?id=6501

competencies. This means that cyber defence is implemented at the national and international level, so the entities must be involved in international security integrations, establish multilateral and bilateral cooperation and actively participate in these integrations (unified approach).[75]

3. National cybersecurity governance

3.1 Governance of the communication networks and systems

The AKOS, as independent national regulatory agency is not indirectly a body for national cybersecurity governance, but regulates and supervises electronic communications market and radio frequency spectrum. Its function as cybersecurity governance is originate indirectly from Electronic Communications Act, under which the AKOS is responsible for the effective development of communication networks and services for the benefit of the population and business entities of Slovenia, promotion of competition, equal operation of electronic communications network and service operators, postal and railway transport service providers, universal service, radio frequency spectrum management, monitoring the content of radio, television programs and audio-visual media services on demand, and protecting the rights of service users.[76]

3.2 Strategic leadership and policy coordination

In accordance with Article 27 of the ZInfV, the highest national strategic cyber security authority is the competent national authority.[77] The Government has established the Information Security Administration of the Republic of Slovenia (ISA) as the competent national body, which is appointed within the Ministry of Public Administration.[78] The ISA as a part of the national security system (Article 22) coordinates the operational capabilities of the information security system and connects stakeholders in the national information security system (Figure 2). Its composition is Common Affairs Sector, Resistance Raising Sector, Strategic Planning and Crisis Response Sector, and Information Society Inspectorate.[79] In addition to other tasks determined by the ZInfV, the ISA has defined the following core tasks (Article 27):

- It is the single point of contact for cross-border cooperation with the relevant authorities of other EU Member States and with the network of CSIRTs and the cooperation group to which it contributes its representative (Figure 2);
- Fulfils other information obligations of the European Commission and the Cooperation Group, information and notification obligations of other international organizations;
- Cooperates with a bodies and an organizations operating in the field of information security, especially with the: national CSIRT and CSIRT of state administration bodies, security and operational centres, regulators or supervisors of areas referred to essential service providers, AKOS, Information Commissioner, law enforcement authorities and providers of security solutions (Figure 2);

[75] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707
[76] AKOS, O agenciji, 2020, https://www.akos-rs.si/o-agenciji, accessed on 2. 12. 2020.
[77] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707
[78] Information Security Administration, Republic of Slovenia, 2020, https://www.gov.si/en/state-authorities/bodies-within-ministries/information-security-administration/, accessed on 2. 12. 2020.
[79] O Upravi Republike Slovenije za informacijsko varnost, Republika Slovenija, 2020, https://www.gov.si/drzavni-organi/organi-v-sestavi/uprava-za-informacijsko-varnost/o-upravi-za-informacijsko-varnost/ accessed on 2. 12. 2020.

- Develops cyber defence capabilities;
- Provides professional support in the field of information security to all subjects liable under the ZInfV;
- Provides analyses, methodological support and preventive action in the field of information security and gives opinions in the field of its competence;
- Makes the subjects liable under the ZInfV aware of the importance of reporting an incident with all the signs of a criminal offense being prosecuted ex officio to the law enforcement authorities in accordance with the Criminal Code;
- Coordinates training, exercises and education in the field of information security and takes care of raising public awareness of information security;
- Encourages and supports research and development in the field of information security;
- Performs testing of information and communication technologies in the field of information security;
- Takes care of the draw and implementation of the strategy;
- Draws up a national incident response plan, taking into account the strategy, the plans of the national CSIRT and CSIRT of state administration bodies, other competent authorities and the safety documentation subjects liable under the ZInfV;
- Reviews the adequacy of the designation of essential service providers and public administration bodies at least every two years and may propose to the Government to update the designations;
- Informs the European Commission at least every two years regarding the tasks arising from the NIS Directive;
- Performs other tasks of international cooperation;
- Performs inspections over the implementation of the ZInfV, as well as controls the compliance of websites and mobile applications under the Website and Mobile Application Accessibility Act (ZDSMA)[80], and the compliance with the regulation in the field of e-identities and trust services (Chapter X of ZInfV).[81]

3.3 Cybersecurity authority and cyber incident response

The National Cyber Security Authority's role and tasks are set out in the ZInfV. It supports the private sector and citizens by sharing information on recent vulnerabilities and coordinating the response to large-scale cyber incidents. In accordance with Article 28 (1), SI-CERT is defined as a **national CSIRT** operating within the public institution ARNES (Academic and Research Network of Slovenia). In exercising its work, the national CSIRT must meet the requirements of a high level of availability of its services, the security of its business premises and business continuity in accordance with the NIS Directive. Its main mission is to respond to cyber incidents at the national level, with the following tasks assigned to it (Article 28 (2)):

- provides methodological support, assistance and cooperation to subject under ZInfV when an incident occurs;
- receives information on risks and vulnerabilities in the field of information security, forwards it to the administrators of the affected systems and publishes warnings;

[80] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o dostopnosti spletišč in mobilnih aplikacij (ZDSMA), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7718

[81] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707; O Upravi Republike Slovenije za informacijsko varnost, Republika Slovenija, 2020, https://www.gov.si/drzavni-organi/organi-v-sestavi/uprava-za-informacijsko-varnost/o-upravi-za-informacijsko-varnost/, accessed on 2. 12. 2020.

- raises awareness of users in the field of information security (SI-CERT is a holder of the national awareness program "Varni na internet" (Safe on internet) and participates in the SAFE.SI project)[82];
- publishes warnings about risks and vulnerabilities in the field of information security;
- cooperates with CSIRTs[83] and security operations centres in the RS and CSIRTs in other EU Member States (Figure 2);
- participates in the network of CSIRTs, and in other international cooperation networks (Figure 2);
- cooperates with the competent national authority and provides it requested information as is identified by ZInfV (Figure 2).[84]

According to Article 29 (2) of ZInfV, the **CSIRT of state administration** bodies (SIGOV-CERT) is responsible for the cyber security at the state administration level. The CSIRT of state administration bodies is operated and coordinated by the Information Security Sector, which is part of the Directorate for Information Society and Informatics of the Ministry of Public Administration with the following tasks:

- receives, processes and evaluates incident notifications within its competence, and records, stores and protects this data;
- provides methodological support, assistance and cooperation to subject under ZInfV when an incident occurs;
- cooperates with the national CSIRT and the competent national authority and, upon request, provides them in a secure manner with information on the exercise of its competences under ZInfV (Figure 2);
- publishes warnings on risks and vulnerabilities in the field of information security of state administration bodies.
- notifies the ISA and national CSIRT of a occurred incident in accordance with Article 18 (3) of the ZInfV (Figure 2).[85]

The incident report is addressed from Articles 13 to 18 of the ZInfV (Figure 2). These Articles identify both security requirements and the immediate reporting of an incident to the national CSIRT if such an incident has a significant impact on the continuing provision of services or a cross-border impact. In addition aforementioned, the national CSIRT must notify the ISA of a reported incident by essential service providers and digital service providers in accordance with Article 13 (3) and Article 14 (4) of the ZInfV. Thus, Article 30 of the ZInfV stipulates cooperation at the national level. This means, that the competent national authority, national CSIRT and CSIRT of state administration bodies may cooperate for the needs of ensuring the national cyber security system, among inter-ministerial, academic-research- development sphere, economy, interest associations and individuals. Additionally, that Article tasking the national CSIRTs and the CSIRTs of public administration bodies to send a quarterly report on the exercising of their task to the competent national authority. In dealing with incidents, Articles 13 to 14 of the ZInfV stipulate reporting of the competent national authority and national CSIRT at the international level (other countries, ENISA, NATO, national Police and National crisis management centre).[86]

[82] O centru SI-CERT, SI-CERT, 2020, https://www.cert.si/o-nas/, accessed on 2. 12. 2020.
[83] There are several CERTs/CSIRTs operating in Slovenia, both in the public and private sectors, however, only two SI-CERT and SIGOV-CERT are accredited or certified by Trusted Introducer, and only SI-CERT is also the member of FIRST. (TF-CSIRT Trusted Introducer, Slovenia, 2020, https://www.trusted-introducer.org/directory/teams.html#url=q%3DSloveni and FIRST, Slovenia, 2020, https://www.first.org/members/map#country%3ASI, accessed on 2. 12. 2020.)
[84] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707
[85] Ibid. Article 20 of the ZInfV also enables the voluntary notification of other incidents by other entities and individuals who are not bound by this Act. (Ibid)
[86] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

According to Article 27 (2) ISA is preparing National Cyber Incident Response Plan. The draft document operationalizes the management of cyber incidents as prescribed in the ZInfV. It prescribes in more detail the levels of cyber incidents, reporting thresholds, reporting time frames and other correlations between cyber security stakeholders at the national level. It also provides procedures for the coordination of the management of the most serious cyber incidents on the national level undertaken by ISA. The draft document was tested on the national part of the Cyber Coalition exercise and it is planned to be formally adopted in the first quarter of next year.[87]

3.4 Cyber crisis management

The ZKI is a lex generalis regarding the protection of critical infrastructure. According to the ZKI shall the critical infrastructure operator, as soon as possible, inform the authority responsible for a critical infrastructure sector and the National Crisis Management Centre (NCKU) of the interruption of the operation of the critical infrastructure for which it has predicted that it may have negative material and other consequences for the functioning of a critical infrastructure sector, and of the already implemented critical infrastructure protection measures. This includes incidents where critical infrastructure is targeted by a malicious cyber operation.[88] The ZInfV as lex specialis regarding information security complements the ZKI, as it stipulates the regulation and provision of security of networks and information systems, which are essential for the smooth functioning of the state and the preservation of key economic and social activities.[89]

The ZInfV stipulates that operators of essential services must without undue delay notify the national CSIRT of the incidents with a significant impact on the continued provision of the essential services. The same provision applies to the national CSIRT who needs to notify ISA and single point of contacts of other states if the incident has cross-border impact. The ISA as a part of national security system connects all stakeholders in the national information security system and coordinates the operational capabilities of the system at a strategic level.[90]

Article 21 of the ZInfV stipulates evaluation of the incident and action. Incidents are classified as minor incident, serious incident and critical incident, and the competent national authority shall immediately notify NSC (and the general public if is needed – Article 23) in the event of a critical incident (including a cyber attack). In the event of a serious and critical incident, the ISA shall immediately issue a decision to the subjects liable under the ZInfV and inform both the government and the NSC. Besides the ones mentioned above, the entities/institutions that are involved in the process of attribution are also other relevant Ministries, most notably the MORS and Ministry of Foreign Affairs, as well as relevant national security agencies such as the SOVA.[91]

In the event of an increase of jeopardy, Article 22 of the ZInfV stipulates that such a situation arises when the probability of a serious or critical event occurring within 72 hours is given. The ISA, in cooperation with other competent authorities, assesses the situation of increased jeopardy and immediately informs the government and the SNC and issues a decision to the subjects liable under the ZInfV to take the necessary measures to prevent or reduce the likelihood of an incident.[92]

[87] Domjanič, M., Email: Review of National CSO Slovenia, 2.12. 2020, ISA.
[88] Uradni list RS, 75/17 (available only in Slovenian), Zakon o kritični infrastrukturi (ZKI), 2017, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7106#
[89] Uradni list RS, št. 30/18 (available only in Slovenian), Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707
[90] Ibid.
[91] Ibid.
[92] Ibid.

Regarding the measures, the RS supports Framework for a joint EU diplomatic response to malicious cyber activities (Cyber Diplomacy Toolbox)[93], and Statement by the North Atlantic Council concerning malicious cyber activities on 3 June 2020[94]. In addition to this, Slovenia together with the EU Member States has so far adopted also two decisions related to restrictive measures: On 30 July 2020 the Council imposed restrictive measures against six individuals and three entities responsible for or involved in various cyber-attacks[95], and on 22 October 2020 the Council imposed restrictive measures on two individuals and one body that were responsible for or took part in the cyber-attack on the German Federal Parliament (Deutscher Bundestag) in April and May 2015.[96]

Slovenia also participates in the Cyber Crisis Liaison Organization Network (CyCLONe) with three representatives (one executive and two officers). The CyCLONe's aim is to contribute to the implementation of the European Commission's Blueprint for rapid emergency response in case of a large-scale cross-border cyber incident or crisis and complement the existing cybersecurity structures at EU level by linking the cooperation at technical (e.g. Computer Security Incident Response Team - CSIRTs) and political levels (e.g. Integrated Political Crisis Response - IPCR).[97]

3.5 Military cyber defence

The development of cyber security in the Slovenian Army (SAF) began in 2003 with the adoption of NATO Directive ACO 70-1[98] by the Ministry of Defence and the SAF. In July 2011, the General Staff of the Slovenian Armed Forces (GŠSV) issued an Order for the implementation of strategic transformation imperatives, and in July 2013, the MoD prepared the concept of cyber defence in the Ministry of Defence. Subsequently, in May 2014, the GŠSV issued an Order on the Establishment of Cyber Security Capabilities, which established a working group to regulate this area. The working group consisted of members of the Intelligence branch (J-2), a member of the Strategic Planning Branch (J-5), members of the Communications and Informatics Branch (J-6) and members of the Communication and Information Systems Unit. Its tasks were the development of cyber capabilities with an emphasis on the system of responding to network and computer incidents, the imposition of new ICTs, international cooperation and the development of education and training. In October 2014, the Order on the Establishment of Cyber Security Capabilities was followed by the Order for Work in the Slovenian Armed Forces for 2015 and 2016. These documents were followed by the establishment of a new cyber security section in J-6 and MIL-CERT was set up as a working group.[99]

---

[93] Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Council of the European Union, 9916/17, 2017, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

[94] Statement by the North Atlantic Council concerning malicious cyber activities, NATO, 2020, https://otan.delegfrance.org/Statement-by-the-North-Atlantic-Council-concerning-malicious-cyber-activities-3, accessed on 2. 12. 2020.

[95] Official Journal of the European Union, L246/12, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN

[96] Official Journal of the European Union, L351I, Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States and Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2020:351I:TOC

[97] Domjanič, M., Email: Review of National CSO Slovenia, 2.12. 2020, ISA.

[98] NATO Directive ACO 70-1 is NATO Allied Command Operations Security Directive. It stipulates minimum standards of information security, encompassing the principles of organization, physical security, communications and computer security, personal security, industrial security and security of information.(Štrucl, D., Pravni in institucionalni vidiki ureditve kibernetske varnosti in obrambe Republike Slovenije, 2020, pp. 28-29, https://revis.openscience.si/IzpisGradiva.php?id=6501)

[99] Štrucl, D., Kibernetska varnost v Republiki Sloveniji in Slovenski vojski, Vojaškošolski zbornik, številka 11, 2016, pp. 114-115, http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/publikacije/VSZ_december2016.pdf

Already in the Medium-Term Defence Program of the Republic of Slovenia 2013-2018 (SOPR 2013-2018), the RS accepted the need to establish cyber security capabilities, and in SOPR 2016-2020 this goal became a priority of the MORS. These priority target capabilities included stationary and mobile cyber defence capabilities at the operational and tactical levels, which has been also confirmed in SOPR 2018-2023.[100]

The current Slovenian legislation does not define cyberspace as the fifth area of warfare or determine the role of the SAF in the event of a cyber attack on the territory of the RS. Thus, the SAF is limited by national law to the cyber defense of its own ICTs. Regardless of that, the RS, as a member of NATO, is a signatory of Cyber Defence Pledge in Warsaw, where it recognizes cyberspace as a new battlefield. Awareness of cyberspace as the fifth domain of warfare is also evident from the NCSS, which was adopted before the signing of mentioned pledge. Therefore, the development of cyber defence capabilities is laid down as the NCSS strategic objective that can independently or in cooperation with the EU and NATO to protect defence ICT systems and provide support to military operations and crisis planning.[101]

In 2020, the White Paper[102] on the Defence was drafted and adopted by Ministry of Defence of the Republic of Slovenia (MORS). The White Paper is a strategic document aimed to present the vision of the long-term development of the functioning of the defence system and achieving key goals in the field of defence by 2035. With these documents and taking into account national legislation, Slovenia reiterates its commitments to NATO and the EU. In the field of cyber defence, the document sets the following objectives: design of a system for comprehensive management of cyber threats of the MORS; develop cooperation with the competent national authority and other actors in the cyber security system; inclusion of the cyber defence capabilities of the Slovenian Armed Forces in the comprehensive system of the MORS and the national system of cyber security and defence; one part of the cyber defence capability will be deployable, etc.[103]

In addition, the Act on the Provision of Funds for Investments in the Slovenian Armed Forces in the Years 2021 to 2026 was adopted as well. By this document Slovenia defines an establishment of a high level of cyber defence and exchange of information with allies[104].

3.6 Engagement with the private sector

In the field of information / cyber security, the Republic of Slovenia formally started financing public projects and cooperating with the academic sphere in 2010, when the Ministry of Public Administration signed an agreement with SI-CERT.[105] As an integral part of ARNES, SI-CERT had taken over the coordination of solving security incidents in the public administration network until 2018, and then took over the role of the national CSIRT, which it still implements. Since 2011, the Ministry of Public Administration and Directorate for the Information Society with the help of EU funds, has been financing numerous information / cyber security projects, such as: Safe on the Internet (Varni na internet[106]), “Safe.si”, TOM telephone (TOM telefon) and Web eye (Spletno oko) (the latter three are run by the Center

[100] Ibid, pp. 112-113.
[101] Cyber Security Strategy, Republic of Slovenia, 2016, p. 15, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf
[102] Bela knjiga o obrambi Reublike Slovenije, Ministrstvo za obrambo, 2020, https://www.gov.si/assets/ministrstva/MO/Dokumenti/BK2020.pdf
[103] Bela knjiga o obrambi Reublike Slovenije, Ministrstvo za obrambo, 2020, https://www.gov.si/assets/ministrstva/MO/Dokumenti/BK2020.pdf
[104] Zakon o zagotavljanju sredstev za investicije v Slovenski vojski v letih 2021 do 2026, ZZSISV26, (available only in Slovenian), Republika Slovenija, 2020, https://www.gov.si/novice/2020-11-20-drzavni-zbor-izglasoval-zakon-za-zagotavljanje-sredstev-za-investicije-v-slovenski-vojski/
[105] Zgodovina spletnih incidentov v Sloveniji, SI-CERT, 2020, https://www.cert.si/o-nas/zgodovina-spletnih-incidentov-v-sloveniji/, accessed on 2. 12. 2020.
[106] O projektu, Varni na internet, 2020, https://www.varninainternetu.si/kdo-smo/, accessed on 2. 12. 2020.

for Safer Internet[107]). In addition to the mentioned ministry and directorate, various faculties, associations, institutes, companies, Supreme State Prosecutor's Office, and the Police are involved in these projects. These projects are primarily intended to raise awareness among the Slovenian public and SME about threats in cyberspace, as well as to prosecute cybercrime.

Engagement with the private sector and academia is also addressed in NCSS, DSI, Next-Generation Broadband Network Development Plan to 2020, Public Administration Development Strategy 2015 – 2020, Research and Innovation Strategy of Slovenia, and the Smart Specialization Strategy. These documents define such cooperation as a strategic goal for increasing the level of information security in state institutions, the economy and the Slovenian public. Thus, Slovenia developed the comprehensive program of digitisation and digital transformation of SMEs 2018-2023, with four measures supported with funds: the activities of the DIH, the Entrepreneurial Fund, a public call for e-business for SMEs, and the public call for digital transformation for SMEs. It is also important to mention nine SRIPT programs, two of which are involving digital technologies:

- SRIP Smart Cities and Communities/ICT Horizontal Network (ICT)[108] and
- SRIP Factories of the future[109] (robotics, photonics, process technologies).[110]

Cooperation between investors, universities, research institutions and ICT providers is carried out within the framework of DIH. This ensures synergies between digital and other technologies and promotes the digitalisation of society. An example of good practice of synergy is the development of the National Strategy for Artificial Intelligence, where the Ministry of Public Administration formed a working group consisting of representatives of various ministries, government departments and external stakeholders, includes: the Slovenian Digital Coalition, Slovenian Society for Artificial Intelligence, Slovenia's Digital Ambassador, the Chamber of Commerce and Industry of Slovenia, Strategic Research and Innovation Partnerships (SRIP PMiS - Smart Cities and Communities and SRIP ToP - Factories of the future), the Jozef Stefan Institute, the Faculty of Computer and Information Science of the University of Ljubljana and others).[111]

[107] O Centru, Safe.si, 2020, https://safe.si/center-za-varnejsi-internet/o-centru, accessed on 2. 12. 2020.
[108] SRIP pametna mesta in skupnosti, Akcijski načrt horizontalna IKT mreža, Fokusno področje: kibernetska varnost, Republika Ministrstvo ta gospodarstvo, razvoj in tehnologijo RS, 2017, http://pmis.ijs.si/wp-content/uploads/2017/03/Akcijski-na%C4%8Drt-Kibernetska-varnost.pdf
[109] SRIP Tovarne prihodnosti, Republika Ministrstvo ta gospodarstvo, razvoj in tehnologijo RS, Ključne usmeritve SRIP Tovarne prihodnosti, 2017, https://www.gzs.si/Portals/222/Klju%C4%8Dne%20usmeritve%20SRIP%20Tovarne%20prihodnosti.pdf
[110] EU, Digital Economy and Society Index (DESI) 2020 Slovenia, 2020a, pp. 10-11, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929. Revision of Slovenia's Smart Specialisation Strategy 2021–2027 is ongoing (more on https://www.teces.si/en/news/revision-slovenia-smart-specialisation-strategy-2021-2027-active-participation-teces.html, accessed on 2. 12. 2020.)
[111] Digital Government Factsheet 2019 Slovenia, European Union, 2019, p. 20, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf

References

Policy

Bela knjiga o obrambi Reublike Slovenije, Mnistrstvo za obrambo, 2020, https://www.gov.si/assets/ministrstva/MO/Dokumenti/BK2020.pdf

Cyber Security Strategy, Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf

Digital Slovenia 2020 – Development Strategy for the Information Society until 2020, Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/Digital-Slovenia-2020-Development-Strategy-for-the-Information-Society-until-2020.pdf

Digitalna Slovenija Načrt razvoja širokopasovnih omrežij naslednje generacije do leta 2020, Republika Slovenija, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/NGO-2020

Enotna metodologija popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi, Ministrstvo za javno upravo, Republika Slovenija, 2019, https://www.gov.si/assets/ministrstva/MJU/DI/Enotna_metodologija_popisovanja_inf_premozenja_in_sistemov_v_DU.pdf

Metodologija obvladovanja tveganj informacijske varnosti v državni upravi, Ministrstvo za javno upravo, Republika Slovenija, 2019, https://www.gov.si/assets/ministrstva/MJU/DI/Informacijska-varnost/Metodologija-obvladovanja-tveganj-informacijske-varnosti-v-drzavni-upravi.pdf

Next-Generation Broadband Network Development Plan to 2020, Republic of Slovenia, 2016, https://www.gov.si/assets/ministrstva/MJU/DID/NGN_2020_Slovenia_EN.pdf

Official Gazette RS, no 59/2019, Resolution of the National Strategy of the Republic of Slovenia, 2019, https://www.gov.si/assets/ministrstva/MO/Dokumenti/ReSNV2.pdf

Public Administration Development Strategy 2015 – 2020, Republic of Slovenia, 2015, https://nio.gov.si/nio/asset/strategija+razvoja+javne+uprave+2015+2020?lang=en

Law

Official Gazette RS, no 57/2000 - Official Consolidated Text and 25/2004) Electronic Commerce and Electronic Signature Act, 2004, http://cyberlawsconsultingcentre.com/wp-content/uploads/2electronic-commerce-and-electronic-signature-act-2000.pdf

Official Gazette RS, no 96/09 - Official Consolidated Text and 19/15) Electronic Commerce Market Act (ZEPT), Unofficial consolidated version No. 4, 2015, http://www.pisrs.si/Pis.web/npbDocPdf?idPredpisa=ZAKO6919&idPredpisaChng=ZAKO4600&type=doc&lang=EN

Official Gazette RS, no 109/12, 110/13, 40/14 - ZIN-B, and 54/14 - Decision of the Constitutional Court no. U-I-65/13 2013, Electronic Communications Act, https://www.legislationline.org/download/id/5561/file/Slovenia_Electronic%20Communications%20Act_2014_en.pdf

Official Journal of the European Union, L246/12, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening

the Union or its Member States, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN

Official Journal of the European Union, L351I, Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States and Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2020:351I:TOC

Uradni list RS, št. 43/04 (available only in Slovenian), Zakon o pogojnem dostopu do zaščitenih elektronskih storitev (ZPDZES), 2004, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3822

Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14, Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), NPB št. 6, 2014, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1973

Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14 in 51/16, 2016, Zakon o državni upravi (ZDU-1), neuradno prečiščeno besedilo 18, 2016, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3225

Uradni list RS, 75/17 (available only in Slovenian), Zakon o kritični infrastrukturi (ZKI), 2017, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7106#

Uradni list RS, št. 62/14 in 13/17, Uredba o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite, NPB št. 1, 2017, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED6795

Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17, Zakon o elektronskih komunikacijah (ZEKom-1), NPB št. 5, 2017, http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6405

Uradni list RS, št. 30/18, Zakon o informacijski varnosti (ZInfV), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

Uradni list RS, št. 30/18, Zakon o dostopnosti spletišč in mobilnih aplikacij (ZDSMA), 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7718

Uradni list RS, št. 39/19 (available only in Slovenian), Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev, 2019, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7808

Uradni list RS, št. 29/18 in 131/20 – NPB št. 1 (available only in Slovenian), Uredba o informacijski varnosti v državni upravi, 2018, http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED7198

Uradni list RS, št. 32/19, 2019, Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev, Republika Slovenija, 2019, http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV13624

Uradni list RS, št. 68/19, Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave, Republika Slovenija, 2019, http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV13669

Zakon o zagotavljanju sredstev za investicije v Slovenski vojski v letih 2021 do 2026, ZZSISV26, (available only in Slovenian), Republika Slovenija, 2020, https://www.gov.si/novice/2020-11-20-drzavni-zbor-izglasoval-zakon-za-zagotavljanje-sredstev-za-investicije-v-slovenski-vojski/, accessed on 2. 12. 2020

Other

BDP in nacionalni računi, Statistični urad, Republika Slovenija, 2020b, https://www.stat.si/StatWeb/Field/Index/1, accessed on 2. 12. 2020

Digitalna družba, Statistical office, Republic of Slovenia, 2020a, https://www.stat.si/StatWeb/Field/Index/25, accessed on 2. 12. 2020

Digital Government Review of Slovenia Leading the digitalisation of the public sector, OECD, 2020, https://www.oecd.org/gov/digital-government/digital-government-review-slovenia-highlights.pdf

Digital Government Factsheet 2019 Slovenia, European Union, 2019, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf

Digital Economy and Society Index (DESI) 2020, 2020, https://eufordigital.eu/wp-content/uploads/2020/06/DESI2020Thematicchapters-FullEuropeanAnalysis.pdf

Digital Economy and Society Index (DESI) 2020 Slovenia, European Union, 2020a, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66929, accessed on 2. 12. 2020

Digital Transformation of Slovenia, Ministry of Public Administration, Republic of Slovenia, 2017, http://www.tirana.embassy.si/fileadmin/user_upload/dkp_55_vti/docs/Digital_transformation_of_Slovenia.pdf

Domjanič, M., Email: Review of National CSO Slovenia, 2.12. 2020, ISA.

Državni računalniški oblak: https://nio.gov.si/nio/asset/drzavni+racunalniski+oblak+dro?, accessed on 2. 12. 2020.

eGovernment in Slovenia, European Commission, January 2015, Edition 18.0, 2015, https://joinup.ec.europa.eu/sites/default/files/inline-files/eGov%20in%20Slovenia%20-%20January%202015%20-%20v_18_0_Final.pdf

E-Government Survey 2020, Digital Government in the Decade of Action for Sustainable Development, United Nations, 2020, https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020 UN E-Government Survey (Full Report).pdf

FIRST, Slovenia, 2020, https://www.first.org/members/map#country%3ASI, accessed on 2. 12. 2020

Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities, Council of the European Union, 9916/17, 2017, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Global Cybersecurity Index (GCI) 2018, International Telecommunication Union (ITU), 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ICT Development Index 2017, International Telecommunication Union (ITU), 2017, https://www.itu.int/net4/ITU-D/idi/2017/index.html, accessed on 2. 12. 2020

Informacijska varnost, Republika Slovenija, 2020, https://www.gov.si/teme/informacijska-varnost/, accessed on 2. 12. 2020

Information Security Administration, Republic of Slovenia, 2020, https://www.gov.si/en/state-authorities/bodies-within-ministries/information-security-administration/, accessed on 2. 12. 2020

Information Society and Informatics Directorate, Republic of Slovenia, 2020, https://www.gov.si/en/state-authorities/ministries/ministry-of-public-administration/about-the-ministry/information-society-and-informatics-directorate/, accessed on 2. 12. 2020

Information technology in public administration, Republic of Slovenia, 2020, https://www.gov.si/en/topics/informatika-v-drzavni-upravi/, accessed on 2. 12. 2020

Kavčič, M., Slovenian National Information Security System under the Information Security Act (December 2020), https://www.gov.si/assets/organi-v-sestavi/URSIV/Datoteke/Dokumenti/Scheme-of-SI-National-Information-Security-System-under-the-ISA.pdf

National Cyber Security Index (NCSI), Slovenia, e-Governance Academy, 2020, https://ncsi.ega.ee/country/si, accessed on 2. 12. 2020

Novice, Republika Slovenija, 2020, https://www.gov.si/novice/2020-09-29-98-dopisna-seja-vlade-republike-slovenije/, accessed on 2. 12. 2020

O agenciji, AKOS, 2020, https://www.akos-rs.si/o-agenciji, accessed on 2. 12. 2020

O centru SI-CERT, SI-CERT, 2020, https://www.cert.si/o-nas/, accessed on 2. 12. 2020

O Centru, Safe.si, 2020, https://safe.si/center-za-varnejsi-internet/o-centru, accessed on 2. 12. 2020

O projektu, Varni na internet, 2020, https://www.varninainternetu.si/kdo-smo/, accessed on 2. 12. 2020

O Upravi Republike Slovenije za informacijsko varnost, Republika Slovenija, 2020, https://www.gov.si/drzavni-organi/organi-v-sestavi/uprava-za-informacijsko-varnost/o-upravi-za-informacijsko-varnost/, accessed on 2. 12. 2020

Ocena kibernetskih tveganj (only in Slovenian) Republika Slovenija, Ministrstvo za javno upravo, 2018, https://www.gov.si/assets/ministrstva/MJU/DI/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf

Poročilo o razvoju trga elektronskih komunikacij za prvo četrtletje 2020, The Agency for Communication Networks and Services of the Republic of Slovenia, 2020, https://www.akos-rs.si/fileadmin/user_upload/Cetrtletno_porocilo_Q1_2020_za_objavo.pdf

Prebivalstvo, Statistični urad, Republika Slovenija, 2020, https://www.stat.si/StatWeb/, accessed on 2. 12. 2020

Prvo 5G omrežje Slovenije, Telekom Slovenije, 2020, https://www.telekom.si/5g, accessed on 2. 12. 2020

Revision of Slovenia's Smart Specialisation Strategy 2021–2027, Teces, 2020, https://www.teces.si/en/news/revision-slovenia-smart-specialisation-strategy-2021-2027-active-participation-teces.html, accessed on 2. 12. 2020

Sloji pokritosti, Geoportal AKOS, 2020, https://gis.akos-rs.si/HomePublic/OPTPogledResult/slo, accessed on 2. 12. 2020

Spremembe v površini zemlje, Statistical office, Republic of Slovenia, 2018, https://www.stat.si/StatWeb/File/DocSysFile/10033/Spremembe_povrsine_Slovenije.pdf

Srednjeročni obrambni program 2018-2023, Vlada Republike Slovenije, 2018, http://84.39.218.201/MANDAT14/VLADNAGRADIVA.NSF/18a6b9887c33a0bdc12570e50034eb54/709feb255697c4b7c125826e00469436/$FILE/SOPR1823Besedilo.docx

SRIP pametna mesta in skupnosti, Akcijski načrt horizontalna IKT mreža, Fokusno področje: kibernetska varnost, Republika Ministrstvo ta gospodarstvo, razvoj in tehnologijo RS, 2017, http://pmis.ijs.si/wp-content/uploads/2017/03/Akcijski-na%C4%8Drt-Kibernetska-varnost.pdf

SRIP Tovarne prihodnosti, Republika Ministrstvo ta gospodarstvo, razvoj in tehnologijo RS, Ključne usmeritve SRIP Tovarne prihodnosti, 2017, https://www.gzs.si/Portals/222/Klju%C4%8Dne%20usmeritve%20SRIP%20Tovarne%20prihodnosti.pdf

Statement by the North Atlantic Council concerning malicious cyber activities, NATO, 2020, https://otan.delegfrance.org/Statement-by-the-North-Atlantic-Council-concerning-malicious-cyber-activities-3, accessed on 2. 12. 2020

Strategija kibernetske varnosti: učinkovit sistem zagotavljanja kibernetske varnosti ni zastonj, Republika Slovenija, 2020, https://www.gov.si/novice/2020-08-05-strategija-kibernetske-varnosti-ucinkovit-sistem-zagotavljanja-kibernetske-varnosti-ni-zastonj/, accessed on 2. 12. 2020

Štrucl, D., Kibernetska varnost v Republiki Sloveniji in Slovenski vojski, Vojaškošolski zbornik, št. 11, 2016, http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/publikacije/VSZ_december2016.pdf

Štrucl, D., Pravni in institucionalni vidiki ureditve kibernetske varnosti in obrambe Republike Slovenije, 2020, https://revis.openscience.si/IzpisGradiva.php?id=6501

TF-CSIRT Trusted Introducer, Slovenia, 2020, https://www.trusted-introducer.org/directory/teams.html#url=q%3DSloveni, accessed on 2. 12. 2020

Zakon o elektronskih komunikacijah, Republika Slovenija, Republika Slovenija, 2020, https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10097, accessed on 2. 12. 2020

Zakonodaja, Ministrstva za javno upravo, Republika Slovenija, 2020, https://www.gov.si/drzavni-organi/ministrstva/ministrstvo-za-javno-upravo/zakonodaja/, accessed on 2. 12. 2020

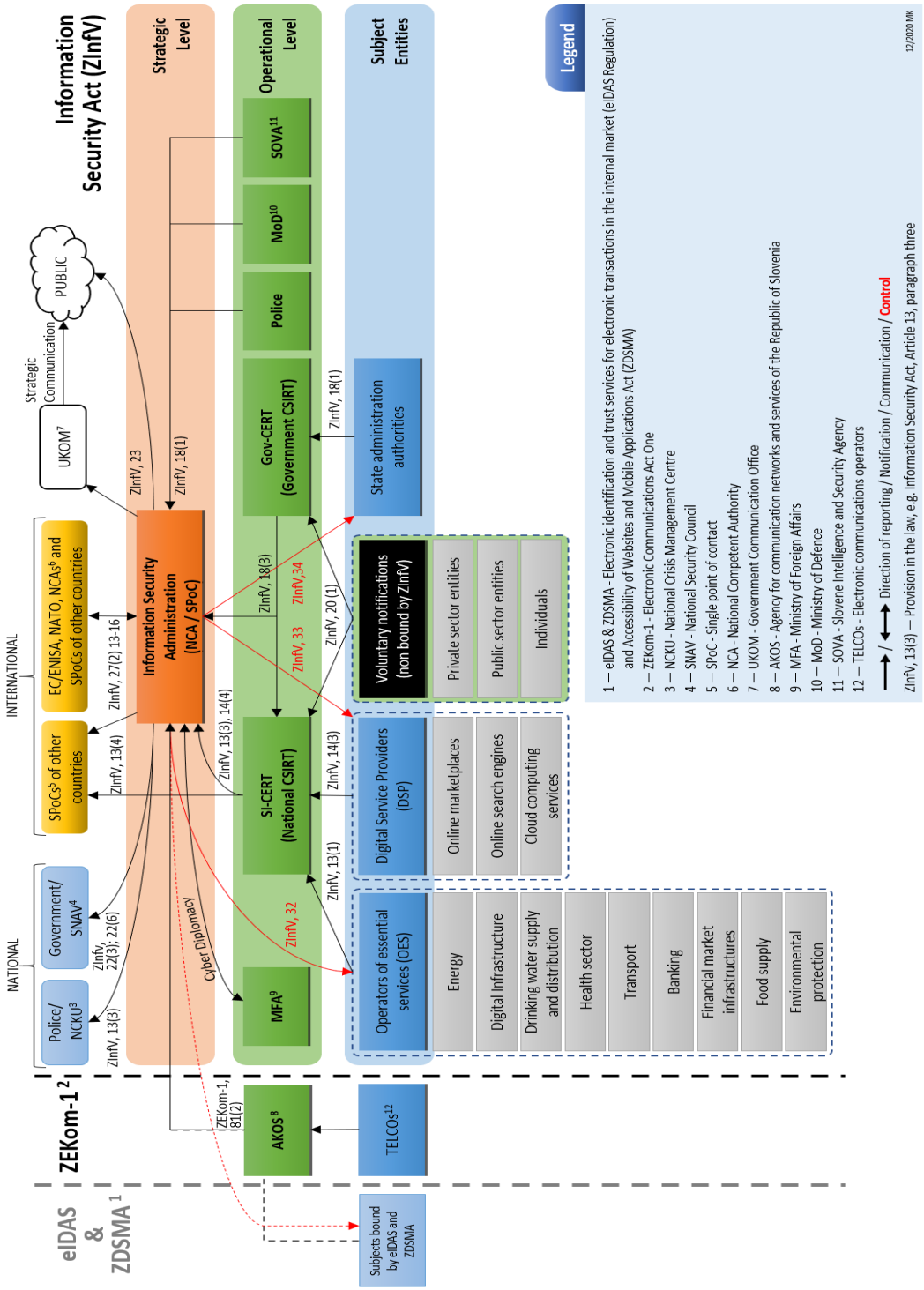
Zgodovina spletnih incidentov v Sloveniji, SI-CERT, 2020, https://www2.cert.si/o-nas/zgodovina-spletnih-incidentov-v-sloveniji/, accessed on 2. 12. 2020

Acronyms

AKOS	Agency for Communication Networks and Services of the Republic of Slovenia
ARNES	Academic and Research Network of Slovenia
CSIRT	Computer security incident response team
DRO	Slovenia State Cloud
DESI	Digital Economy and Society Index
DIH	Digital Innovation Hubs
DSI	Digital Slovenia Strategy
ENISA	European Cybersecurity Agency
EU	European Union
GŠSV	General Staff of the Slovenian Armed Forces
ICT	Information Communication Technology
ISA	Information Security Administration / Competent National Authority
IT	Information Technology
ITU	International Telecommunication Union
MORS	Ministry of Defence of the Republic of Slovenia
NCS	National Security Council
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
RS	Republic of Slovenia
SAF	Slovenian Armed Forces
SI-CERT	Slovenian National Cyber Security Incident Response Centre
SIGOV-CERT	Slovenian Governmental Computer Emergency Response Team
SME	Small and Medium-Sized Enterprise
SOPR	Medium-Term Defense Program of the Republic of Slovenia
SOVA	Slovenian Intelligence and Security Agency
ZInfV	Information Security Act
ZKI	Critical infrastructure Act

Appendix

Figure 2: Slovenian National Information Security System under the Information Security Act[112]



[112] Kavčič, M., Slovenian National Information Security System under the Information Security Act (December 2020), https://www.gov.si/assets/organi-v-sestavi/URSIV/Datoteke/Dokumenti/Scheme-of-SI-National-Information-Security-System-under-the-ISA.pdf