



Slovenian case study on cybersecurity technology and information transfer

Work package	WP4 Know-how, good practice sharing, and information transfer activities
Task	T4.1. National Case Studies
Due date	20-11-2025
Submission date	30-11-2025
Deliverable lead	ULB
Version	v1.0
Authors	CCIS, Slovenia
Reviewers	WP4 partners

Abstract

This case study examines Slovenia’s cybersecurity landscape, focusing on technology transfer, information sharing, and cooperation between civil and defence sectors. The research, based on desk analysis, interviews, surveys, and expert validation, finds that while Slovenia has established a solid regulatory and institutional foundation aligned with EU standards, implementation remains uneven. Key challenges include fragmented coordination, insufficient funding, and a shortage of skilled professionals. Nonetheless, strong progress has been achieved in international cooperation, R&D participation, and the development of national capabilities such as SI-CERT and URSIV. The study highlights the need to update the national cybersecurity strategy, enhance technology transfer mechanisms, and strengthen dual-use innovation. It concludes that Slovenia’s resilience depends on sustained political commitment, trust-based collaboration, and the integration of research, industry, and public administration into a coherent cybersecurity ecosystem.

Keywords

Cybersecurity, Technology transfer, Information sharing, Dual-use, Public–Private Partnership, National cybersecurity strategy, Research and development, Innovation, Civil–defence cooperation, Policy recommendations, Slovenia, Digital resilience

Document revision history

Version	Date	Description of change	Contributor(s)
v.0.1	08-04-2025	Draft table of contents	CCIS, Slovenia
v.0.2	19-09-2025	Draft, including desk research and interviews	CCIS, Slovenia
v.0.3	30-10-2025	Draft, integrating surveys	CCIS, Slovenia
v.0.4	06-11-2025	Draft, integrating workshop	CCIS, Slovenia
v.0.5	07-11-2025	Draft, conclusions	CCIS, Slovenia
v.1.0	10-11-2025	Final, revision of v.0.5	CCIS, Slovenia

Disclaimer

The COcyber project funded under Grant Agreement No. 101158606 is supported by the European Cybersecurity Competence Centre and funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

Copyright notice

© COcyber 2024-2026

Project funded by the European Commission in the Digital Europe Programme

Nature of the deliverable	R
Dissemination level	
Public – fully open. e.g., website	✓
Sensitive (SEN) – limited under the conditions of the Grant Agreement	
EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444	

Table of Contents

TABLE OF CONTENTS 4

LIST OF ABBREVIATIONS AND ACRONYMS7

EXECUTIVE SUMMARY12

1 INTRODUCTION.....13

1.1 BACKGROUND AND CONTEXT OF CYBERSECURITY TECHNOLOGY AND INFORMATION TRANSFER13

1.2 OBJECTIVES OF THE CASE STUDY15

1.3 SCOPE AND LIMITATIONS16

2 METHODOLOGY.....16

2.1 RESEARCH METHODS.....17

2.1.1 Desk research.....17

2.1.2 Semi-structured stakeholder interviews17

2.1.3 Online stakeholder survey18

2.1.4 National experts’ validation workshop19

2.2 DATA ANALYSIS AND REPORTING20

3 NATIONAL CYBERSECURITY LANDSCAPE..... 20

3.1 OVERVIEW OF NATIONAL CYBERSECURITY POLICIES AND STRATEGIES.....20

3.2 MAIN STAKEHOLDERS IN THE COUNTRY 23

3.3 NATIONAL CYBERSECURITY CHALLENGES AND GAPS..... 26

3.4 INTERNATIONAL COOPERATION AND PARTNERSHIPS IN CYBERSECURITY RESEARCH..... 28

4 TECHNOLOGY TRANSFER FRAMEWORK31

4.1	DEFINITION AND IMPORTANCE OF TECHNOLOGY TRANSFER IN CYBERSECURITY	32
4.2	LEGAL AND REGULATORY FRAMEWORK GOVERNING TECHNOLOGY TRANSFER RESEARCH	34
4.3	NATIONAL INSTITUTIONS RESPONSIBLE FOR FACILITATING TECHNOLOGY TRANSFER	38
4.4	INCENTIVES AND BARRIERS TO TECHNOLOGY TRANSFER	42
4.5	EXAMPLES OF SUCCESSFUL TECHNOLOGY TRANSFER INITIATIVES	46
5	INFORMATION SHARING MECHANISMS	48
5.1	EXISTING NATIONAL CYBERSECURITY INFORMATION-SHARING POLICIES AND FRAMEWORKS	49
5.2	CYBERSECURITY THREAT INTELLIGENCE SHARING MECHANISMS, PLATFORMS AND TOOLS (E.G., CERTs, ISACs) 52	
5.3	INTERNATIONAL COOPERATION AND BEST PRACTICES IN CYBERSECURITY INFORMATION SHARING	54
5.4	CHALLENGES IN CROSS-SECTORAL INFORMATION SHARING	57
5.5	OTHER INFORMAL INFORMATION AND KNOWLEDGE SHARING INSTRUMENTS	58
6	ANALYSIS OF DUAL-USE TECHNOLOGIES	60
6.1	DEFINITION AND IMPORTANCE OF DUAL-USE CYBERSECURITY TECHNOLOGIES	60
6.2	NATIONAL POLICIES AND FRAMEWORKS GOVERNING DUAL-USE CYBERSECURITY SOLUTIONS	62
6.3	CHALLENGES IN REGULATING AND MANAGING DUAL-USE TECHNOLOGIES	64
6.4	EXAMPLES OF CYBERSECURITY TECHNOLOGIES WITH DUAL-USE APPLICATIONS	66
7	POLICY RECOMMENDATIONS	67
7.1	STRENGTHENING NATIONAL CYBERSECURITY GOVERNANCE	68
7.2	ENHANCING TECHNOLOGY TRANSFER MECHANISMS	69
7.3	IMPROVING INFORMATION SHARING PRACTICES	70
7.4	MANAGING DUAL-USE CYBERSECURITY TECHNOLOGIES	71
8	CONCLUSIONS	72
9	ANNEXES	73

9.1	REFERENCES AND BIBLIOGRAPHY	73
9.2	LIST OF RELEVANT ORGANISATIONS, INITIATIVES, AND PROJECTS MENTIONED IN THE DOCUMENT	76
9.3	BACKGROUND LITERATURE	79
9.4	ANNEX 1 – IN-DEPTH INTERVIEW QUESTIONNAIRE	79
9.5	ANNEX 2 – ONLINE SURVEY	82
9.6	ANNEX 3 – QUESTIONS TO GUIDE THE NATIONAL VALIDATION WORKSHOPS	86

List of abbreviations and acronyms

Abbreviation	Description
AI4SI	Artificial Intelligence for Slovenia – non-profit think tank and platform of SRIP GoDigital promoting, coordinating and organising efficient knowledge transfer from AI research to implementation in companies and organisations.
AKOS	Agency for Communication Networks and Services of the Republic of Slovenia – national regulatory authority for electronic communications and digital services
AMETIC	The Chamber of Commerce and Industry of Slovenia, COcyber partner leading the synergies with existing initiatives, exploitation and sustainability (WP6), and responsible for the National Case Study Report of Spain (WP4).
ARIS	Slovenian Research and Innovation Agency – funds research and innovation projects, integrating technology transfer elements
ARSC2EX 24	Adriatic Regional Cyber Cooperation Exercise
AUS	AUSTRALO marketing lab, COcyber partner leading communication, dissemination and stakeholder engagement (WP5).
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence – multinational cyber defence hub based in Tallinn, Estonia
CCIS	The Chamber of Commerce and Industry of Slovenia, COcyber partner responsible for the National Case Study Report of Slovenia (WP4).
CERT	Computer Emergency Response Team, a group of information security experts who identify, analyse and mitigate cybersecurity incidents and threats.
CRA	Cyber Resilience Act – EU regulation establishing cybersecurity requirements for digital products and software
CRRT	Cyber Rapid Response Teams and Mutual Assistance in Cyber Security – EU initiative under PESCO enabling the rapid deployment of multinational cyber response teams and mutual assistance mechanisms.
CSIRT	Computer Security Incident Response Team – technical team for handling cybersecurity incidents
CTF	Catch the Flag
CTI	Cyber threat intelligence
CyberHubs	European Network of Cybersecurity Skills Hubs – Erasmus+ project aiming to establish a sustainable network of seven cybersecurity skills hubs across Europe.
CyberSEAS	Cyber Securing Energy Data Services – EU-funded project enhancing cybersecurity and resilience of European energy systems and supply chains.
DEP	Digital Europe Programme, funding instrument of the European Union.

DORA	EU Digital Operational Resilience Act
DOVOS	State-owned Defence, Security and Resilience Company of Slovenia
EC	The European Commission, the European public authority funding the COcyber project.
ECC	The European Cybersecurity Competence Centre, the funding authority of the COcyber project.
ECSSO	European Cyber Security Organisation
EDA	European Defence Agency – supports EU Member States in developing defence capabilities
EDF	European Defence Fund – EU financial instrument supporting collaborative defence R&D
EDIH	European Digital Innovation Hub – EU-supported centre promoting digital transformation and cybersecurity adoption
EITD	EIT DIGITAL, COcyber coordinator leading project management (WP1) and synergies (WP6).
ENISA	European Union Agency for Cybersecurity – EU centre of expertise for cybersecurity policy, certification, and operations
EOS	The European Organisation for Security, COcyber partner leading Coordination activities between cybersecurity civilian and defence spheres (WP2).
EU	The European Union (EU) is a political and economic union of 27 European countries, designed to foster economic cooperation, promote peace, and create a single market with free movement of goods, services, and people.
GDPR	General Data Protection Regulation – EU regulation governing data protection and privacy
GOIS	Defence and Protection Cluster of Slovenia
ICS	Institute for Corporate Security Studies – Slovenian research institute focused on security and defence
ICT	Information and Communication Technology
INFOBALT	The Digital technology sector association of Lithuania, COcyber partner responsible for the National Case Study Report of Lithuania (WP4).
IoC	Indicators of compromise
IP	Intellectual property
ISACA	Information Systems Audit and Control Association
ISACs	Information Sharing and Analysis Centres, non-profit organisations that provide a central resource for gathering information on cyberthreats.
IVSZ	The Information and Communication Technologies industry association of Hungary, COcyber partner responsible for the National Case Study Report of Hungary (WP4).
JSI	Jožef Stefan Institute – Slovenian public research organisation in science and technology

LC	The Lisbon Council, COcyber partner leading Cybersecurity Observatory & COcyber Platform (WP3).
MDP	Ministry of Digital Transformation (Slovenia)
MeliCERTes	Member States' CERTs cooperation platform – EU platform supporting cross-border cooperation and information exchange among national and governmental CSIRTs.
MGTS	Ministry of the Economy, Tourism and Sport (Slovenia)
MISP	Malware Information Sharing Platform – open-source system for structured threat intelligence exchange
MKRR	Ministry of Cohesion and Regional Development (Slovenia)
MoD/MORS	Ministry of Defence of the Republic of Slovenia
MVZI	Ministry of Higher Education, Science and Innovation (Slovenia)
NATO	NATO (North Atlantic Treaty Organization) is a military alliance formed in 1949, consisting of 30 member countries from Europe and North America, aimed at ensuring collective defence and security against common threats. It operates under the principle that an attack on one member is an attack on all.
NATO DIANA	Defence Innovation Accelerator for the North Atlantic – NATO innovation programme supporting dual-use technologies and start-ups in defence and security.
NCC / ECC	National Cybersecurity Coordination Centre / European Cybersecurity Competence Centre – national and European coordination bodies forming the EU Cybersecurity Competence Network under Regulation (EU) 2021/887.
NCC-SI	National Coordination Centre for Cybersecurity – Slovenian hub within the EU Cybersecurity Competence Network
NIS2	EU Directive on Security of Network and Information Systems – updated legal framework for cybersecurity across the EU
PESCO	Permanent Structured Cooperation – EU defence initiative
PPP	Public-Private Partnership – cooperative arrangement between public authorities and private organisations
R&D	Research and Development
RDI	Research, Development and Innovation
ReDPROSV40	Resolution on the General Long-Term Development and Equipping Programme of the Slovenian Armed Forces until 2040
ReSNV-2	Resolution on the National Security Strategy of the Republic of Slovenia
SeKV	Sekcija za kibernetsko varnost is the cybersecurity working group within the ICT Association of Slovenia (ZIT) at CCIS
SEN	Sensitive – dissemination level under EU Grant Agreement terms
SI-CERT	Slovenian Computer Emergency Response Team – national cyber incident response authority
SIDEC 2025	The first International Defence Exhibition and Conference in Slovenia

SIEM	Security Information and Event Management
SIGOV-CERT	Governmental Computer Emergency Response Team – handles cybersecurity within Slovenian public administration
SIKV	The Information & Cyber-Security Division (SIKV) inside URSIV
SME	Small and Medium-sized Enterprise – a business of limited size and scale, as defined by the European Commission.
SOC	Security Operations Center
SOPR 2023–2028	Medium-term Defence Programme of the Republic of Slovenia (2023–2028)
SOVA	Slovenian Intelligence and Security Agency (Slovenska obveščevalno-varnostna agencija)
SPIRIT	Public Agency for Entrepreneurship, Internationalization, Foreign Investments and Technology of Slovenia
SPS	Slovene Enterprise Fund (Slovenski podjetniški sklad) – national SME and start-up funding body
SRIP	Strategic Research and Innovation Partnership – national cluster linking academia and industry in priority areas
STI	Science, Technology and Innovation
STIX	Structured Threat Information eXpression – OASIS standard for modelling and serialising cyber threat intelligence (CTI) data, such as indicators, entities, relationships and TTPs.
TAXII	Trusted Automated eXchange of Indicator Information – OASIS application protocol for the exchange of CTI over HTTP(S) (e.g. TAXII 2.1 API, collections, channels).
TLP	Unified trust levels
TRL	Technology Readiness Levels
TTO	Technology Transfer Office – organisational unit managing the commercialisation of research results
TTP	Tactics, Techniques and Procedures – Standard framework for describing adversary behaviour within cyber threat intelligence.
ULB	Université Libre de Bruxelles Solvay Brussels School, COcyber partner leading Know-how, good practice sharing, and information transfer activities (WP4).
URSIL	Slovenian Intellectual Property Office
URSIV	Government Information Security Office of the Republic of Slovenia (Urad Vlade za informacijsko varnost)
WP	Work Package, form the COcyber working process.
ZAG	Slovenian National Building and Civil Engineering Institute
ZEKom-1	Electronic Communications Act
ZGD-1	Companies Act provides the legal framework for establishing companies

ZInfV / ZInfV-1	Information Security Act – Slovenian law transposing the EU NIS2 Directive into national legislation
ZJN-3	Public Procurement Act supports technology transfer indirectly by enabling mechanisms
ZNIBDR	Dual-Use Goods Export Control Act, regulates the export of goods, software, and technology with both civilian and military applications
ZNIBOMN	Defence-Related Goods Export Control Act, focuses specifically on military equipment and defence-related technologies
ZRISS 2030	Resolution on the Slovenian Scientific Research and Innovation Strategy 2030
ZViS	Higher Education Act
ZZrID	Law on Scientific Research and Innovation Activities (Zakon o znanstvenoraziskovalni in inovacijski dejavnosti)

Executive summary

This report presents the Slovenian case study within the COcyber project, analysing the national landscape of cybersecurity technology and information transfer. It examines how Slovenia's institutional, legislative, and innovation frameworks support the interaction between civil and defence stakeholders in strengthening national and European resilience.

The study combines desk research, interviews, and expert consultations to map key actors, identify challenges, and highlight opportunities. It finds that Slovenia has a well-established legal and institutional foundation aligned with EU standards, supported by active institutions such as SI-CERT, URSIV, and the NCC-SI. However, several structural barriers remain, including fragmented coordination, limited technology transfer capacity, and a shortage of cybersecurity professionals. There is a prevailing view among participants that improving cooperation is essential for ensuring national cyber resilience, as well as an opportunity for further development of the digital society.

The findings show broad agreement regarding numerous achievements — including progress in the regulatory framework, the functioning of the central Government Information Security Office (URSIV) and the national SI-CERT, the intensive development of R&D projects within the Ministry of Defence (MORS), successful development projects, and exemplary cooperation in cybersecurity exercises.

The study provides a detailed analysis of the regulatory framework, which is extensive and complex, particularly due to the inclusion of European legislation with binding legal force. It also analyses the obstacles to more effective technology transfer, information sharing, and the intensified development of dual-use products. These barriers have been examined and addressed with the aim of preparing concrete proposals and detailed policy recommendations.

The findings are also unanimous in recognising the urgent need to renew the national strategy, which must define clear and measurable objectives and assign responsibilities to both state and industry stakeholders. The cybersecurity development programme should significantly strengthen active cooperation at both strategic and operational levels and address open questions concerning the development of national capabilities in public institutions and industry. It should also ensure coherent collaboration in research, development, and innovation, technology transfer, information sharing, development of dual-use products, skills and workforce development, resilient digital infrastructure, and optimal international cooperation — all supported by stable financial resources for implementation.

The study concludes with clear recommendations by all stakeholders in the cybersecurity ecosystem. It emphasises that progress can only be achieved through active cooperation, as cybersecurity is a complex, interconnected domain where no single organisation can tackle all challenges on its own.

1 Introduction

This section introduces the purpose and scope of the Slovenian case study, providing context on the importance of cybersecurity technology, information transfer in the national landscape and civil defence collaboration. It outlines the rationale for conducting the study, the key questions it seeks to address, and the methodologies used to gather and analyse data.

1.1 Background and context of cybersecurity technology and information transfer

Cybersecurity has become a cornerstone of national security and economic stability. As digital infrastructures expand, the need for robust cybersecurity measures and effective information sharing becomes paramount. Technology, including dual-use technologies with both civilian and defence applications, is key to moving innovations from research into real-world use—enhancing the ability to prevent, detect, and respond to cyber threats.

Given limited resources and funding, coordinated efforts and international collaboration are essential. Sharing information about threats, vulnerabilities, and best practices across borders helps build a collective defence against cyber adversaries. At the national level, coordinated efforts among government agencies, private sector entities, and academic institutions are essential for developing and implementing effective cybersecurity strategies.

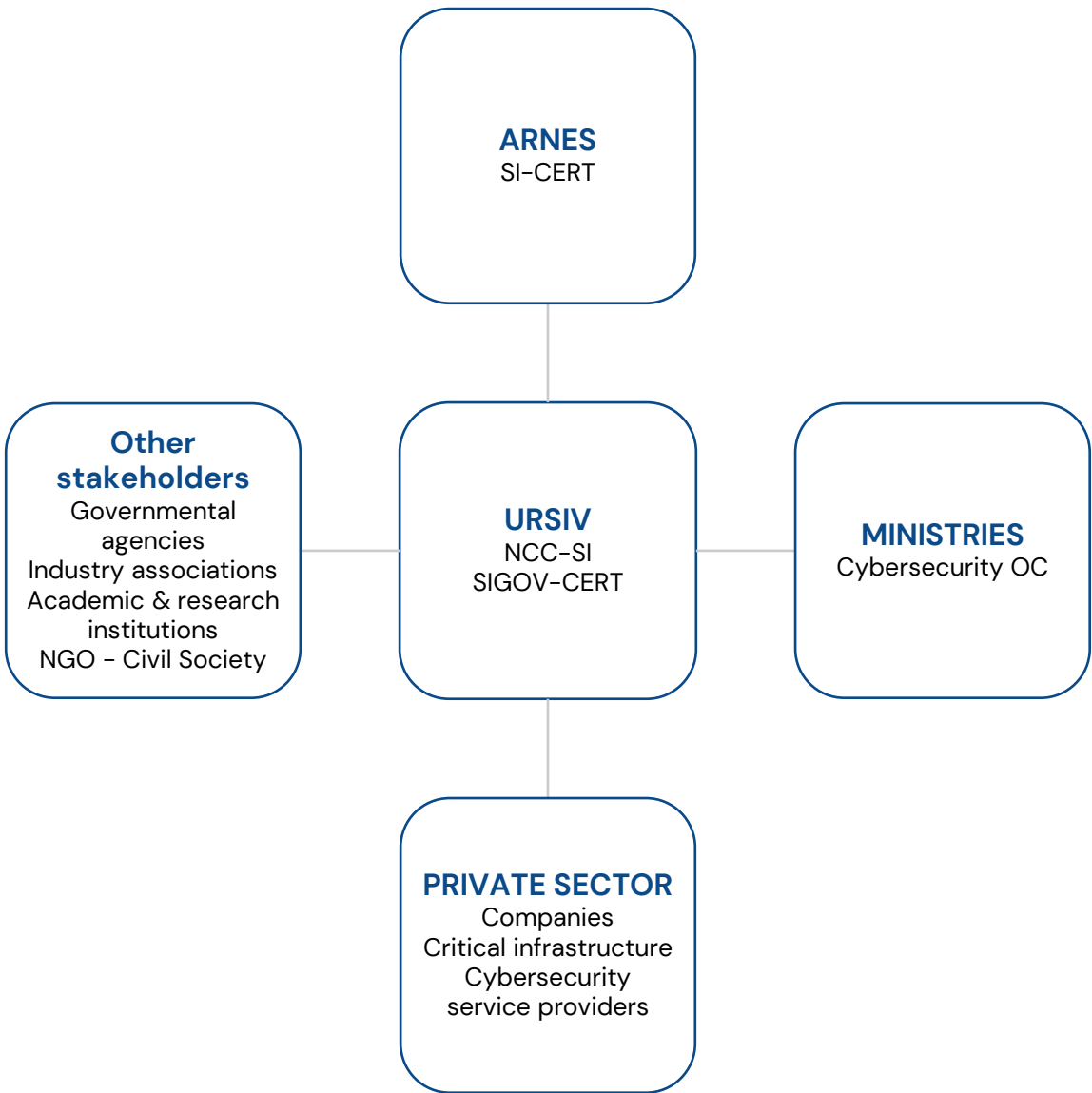


Figure 1: Slovenian cybersecurity stakeholder map

Slovenia’s cybersecurity landscape is steadily evolving in response to rapid digitalisation and the growing complexity of cyber threats. The country has aligned itself with key European frameworks, including the NIS2 Directive (enforced in May 2025) and GDPR, reinforcing its commitment to a secure digital environment. The national cybersecurity ecosystem consists of a diverse range of stakeholders—public institutions, critical infrastructure operators, industry associations, private companies, academia, NGOs, and cybersecurity service providers. Coordination is supported by structured mechanisms such as mandatory incident reporting to national bodies like SI-CERT and SIGOV-CERT, while URSIV (Government Information Security Office) oversees policy implementation. The NCC-SI (National Coordination Centre for Cybersecurity) plays a key role in national and EU-level coordination, supporting research, innovation, and knowledge-sharing.

However, while this framework is just established, more consistent cross-sector collaboration remains a priority—especially between civilian and defence stakeholders.

Slovenia's formal adoption of NIS2 into national law in 2025 marks a significant milestone, aligning the country with the latest EU standards for cybersecurity governance. Nonetheless, some areas require renewed focus—Slovenia's national cybersecurity strategy has not been updated since 2016, and the Digital Strategy provides only limited provisions and funding for cybersecurity. Most financial support currently stems from EU programmes and recent defence-driven initiatives targeting dual-use cybersecurity capabilities. These developments highlight the urgency—and opportunity—to modernise national strategies, leverage EU partnerships, and unlock the full potential of cross-sector collaboration.

In the current cybersecurity landscape, technology transfer and structured information sharing are vital to strengthening national cyber resilience. Slovenia has made progress in fostering cooperation across sectors, but challenges remain—particularly in the dual-use domain, where civilian and defence sectors shall establish much closer collaboration. The effective transfer of cybersecurity technologies and practices across these spheres could enhance threat detection, response capabilities, and innovation. At present, limited communication and siloed operations hinder the full potential of this synergy. National participation in EU and international initiatives—such as ECSO, ENISA, CCDCOE, NATO's LockedShields, Women4Cyber, and organizations like DigitalEurope—along with NCC-SI's collaboration within the European Cybersecurity Competence Network, offers useful channels to address these challenges. Additionally, the COcyber project provides a timely opportunity to promote stakeholder engagement and support more integrated approaches to cybersecurity at both national and European levels. It addresses urgent needs such as dual-use innovation, and strategic alignment across sectors.

1.2 Objectives of the case study

The primary objective of this case study is to analyse and enhance the mechanisms of cybersecurity technology transfer, innovation, and information sharing within Slovenia, contributing to the broader goals of the COcyber project.

The specific objectives of the Slovenia are:

- Identify and document current national frameworks, policies, and practices related to cybersecurity technology transfer, information sharing and dual use.
- Identify key stakeholders across government, industry, academia, civil society, and the military sphere, involved in cybersecurity initiatives.

- Evaluate the effectiveness of existing mechanisms for technology transfer and information sharing, highlighting strengths and areas for improvement.
- Analyse challenges and barriers hindering effective cybersecurity collaboration and propose solutions to overcome them.
- Formulate actionable policy recommendations to enhance national cybersecurity resilience through improved technology transfer and information sharing.

1.3 Scope and limitations

This case study focuses on the national mechanisms for cybersecurity technology transfer and information sharing, examining the roles of various stakeholders, including government bodies, private sector organizations, and academic institutions. The study encompasses policies, frameworks, and practices currently in place, as well as recent initiatives aimed at enhancing these processes.

Some limitations of this case study are:

- The study is confined to publicly available information and data obtained through stakeholder interviews and surveys validated by expert group panel.
- It does not delve into classified or sensitive information that is not accessible through open sources.
- The findings are based on the current state of affairs and may not account for rapidly evolving cybersecurity threats or technologies.
- Additionally, a significant limitation for the scope of this study is the timeline: only data up to the November 2025 is considered. This temporal boundary ensures that the analysis remains focused on information collected, actions and initiatives within the defined period, providing also a precise framework for evaluating progress and challenges.

2 Methodology

The national case studies adopt a mixed-method approach combining desk research, semi-structured interviews, an online survey, and a national expert validation workshop. This approach ensures comprehensive evidence collection and validation across Spain, Lithuania, Slovenia, and Hungary.

2.1 Research methods

This section outlines the methodological framework employed in the COcyber national case studies to investigate cybersecurity technology transfer and information-sharing mechanisms within Spain, Lithuania, Slovenia, and Hungary. A mixed-methods approach was adopted to ensure a comprehensive understanding of each country's cybersecurity landscape, facilitating both depth and breadth in data collection and analysis.

The research design encompasses four key components:

- Desk research: An extensive review of national cybersecurity strategies, policies, legal frameworks, and academic literature was conducted to establish a foundational understanding of each country's cybersecurity environment.
- Semi-structured interviews: Targeted interviews with key stakeholders—including representatives from government agencies, private sector entities, academic institutions, and civil society organisations—were carried out to gather in-depth qualitative insights.
- Online survey: A structured survey was disseminated to a broader group of stakeholders to collect quantitative data and validate findings from the interviews and desk research.
- National validation workshops: Each country hosted a workshop with at least 15 experts to review preliminary findings, ensuring the accuracy and relevance of the data and interpretations.

This multi-faceted methodology was designed to capture a holistic view of cybersecurity practices and challenges in each nation, providing a robust basis for comparative analysis and policy recommendations.

2.1.1 Desk research

A preliminary literature review and policy analysis were conducted at the national level. This phase includes the review of:

- National cybersecurity strategy and policies
- Legislation and regulatory frameworks
- Existing technology transfer and information-sharing mechanisms
- Relevant academic and industry publications

2.1.2 Semi-structured stakeholder interviews

Using a common interview guide, a series of in-depth interviews were carried out with national stakeholders.

Stakeholder categories include:

- Government agencies and regulators
- Private sector representatives (including critical infrastructure operators)
- Research and academic institutions
- Civil society or industry associations
- Military-related organisations

The target was to interview at least 2 stakeholders per category.

The study involved:

Stakeholder category	Number of interviews
Government agencies and regulators	3
Private sector representatives	4
Research and academic institutions	3
Civil society or industry associations	4
Military-related organisations	4
Total	18

Table 1: Number of interviews per stakeholder category

2.1.3 Online stakeholder survey

An online survey was distributed to a broader set of mapped stakeholders in each country. This survey aims to:

- Reach a wider audience beyond direct interviews
- Validate preliminary findings
- Collect additional quantitative or qualitative insights

The study involved:

Stakeholder category	Number of survey responses
Government agencies and regulators	3
Private sector representatives	9
Research and academic institutions	3
Civil society or industry associations	3
Military-related organisations	3
Total	21

Table 2: Number of survey responses per stakeholder category

2.1.4 National experts' validation workshop

A national validation workshop will be organised in each country in early October 2025, gathering at least 10 national experts.

The objectives are:

- To present and validate the draft findings
- To gather final inputs and ensure stakeholder alignment
- To refine recommendations based on multi-sectoral expert feedback

The expert panel involved:

Stakeholder category	Number of participants
Government agencies and regulators	0
Private sector representatives	2
Research and academic institutions	1
Civil society or industry associations	3
Military-related organisations	4
Total	10

Table 3: Number of participants in expert panel per stakeholder category

2.2 Data analysis and reporting

Data gathered through desk research, interviews, and the online survey were analysed thematically and synthesised into draft case study reports. The findings were validated through the national workshops before finalising the deliverables.

3 National cybersecurity landscape

This section examines the Slovenian's existing cybersecurity framework, policies, and key stakeholders with an emphasis on activities between cybersecurity civilian and defence spheres. It identifies the legal and regulatory landscape, as well as the institutions responsible for overseeing cybersecurity efforts. It also examines key aspects of the national cybersecurity landscape, including current practices, opportunities for enhancement, and areas of strategic focus.

3.1 Overview of national cybersecurity policies and strategies

Key strategies, legislative and policy documents are:

- The Digital Slovenia 2030 Strategy (Government of the Republic of Slovenia, 2023a) sets out the country's long-term vision for digital transformation, focusing on inclusive digital society, competitive digital economy, and secure, resilient digital infrastructure. It highlights the importance of cybersecurity as a cross-cutting enabler.
- The Resolution on the National Security Strategy (ReSNV-2) (Government of the Republic of Slovenia, 2019) is the overarching framework for Slovenia's security policy, identifying national interests, threats, and systemic responses. It highlights hybrid threats, cyber operations, and disinformation as major challenges, underlining the importance of timely information exchange and coordination across government, defence, intelligence, and civilian stakeholders.
- National Cyber Security Strategy of the Republic of Slovenia) (Government of the Republic of Slovenia, 2016) outlines the country's foundational approach to securing cyberspace. It emphasizes the protection of critical infrastructure, improved governance and coordination, development of CSIRTs, public awareness and professional training, and international cooperation within the EU and NATO frameworks.

- ZInfV-1 (Zakon o informacijski varnosti – 1) (Republic of Slovenia, 2025) is Slovenia's Information Security Act, updated to align with the EU's NIS-2 Directive. It provides the legal framework for cybersecurity across critical sectors, ensuring risk management, incident reporting, and security standards for essential and important service providers.
- The Resolution on the General Long-Term Development and Equipping Program of the Slovenian Armed Forces until 2040 (ReDPROSV40) (Ministry of Defence of the Republic of Slovenia, 2020) is the highest development-guiding and long-term planning document for development and equipping of the Slovenian Armed Forces. The 2025 update elevates cyber defence as a core investment pillar, alongside kinetic forces and logistics, and emphasizes digitalization and non-kinetic capabilities. It formalizes dual-use investments in cyber, transport, health, and energy to strengthen national resilience, within a two-pillar model that distinguishes core defence spending (targeting 3% of GDP by 2030) from broader security infrastructure.
- Medium-term Defence Programme of the Republic of Slovenia 2023–2028 (SOPR 2023–2028) (Ministry of Defence of the Republic of Slovenia, 2023) outlines ambitious goals: to upgrade current cyber capabilities with a cyber training ground already in place, a monitoring and response capability, and a capability to research threats and vulnerabilities in cyberspace. To strengthen the cyber resilience of our own CIS and contribute to a comprehensive system of national cybersecurity and alliances, the program also envisages cooperation with industry.

The National cybersecurity strategy was an important milestone in establishing the fundamental conditions for the development of this field in Slovenia. It laid the foundation for an institutional framework, including the creation of the Government Information Security Office (URSIV), which contributed to greater transparency of responsibilities and better coordination among stakeholders. Progress has been made in certain areas, especially in organizational arrangements and operational responses to incidents, particularly in connection with critical infrastructure, public safety, defence capabilities, and, to some extent, the economy. Participants acknowledge that, through these efforts, Slovenia has put in place the basic mechanisms for building resilience and has become integrated into European and Euro-Atlantic structures and professional networks. This represents a positive step towards stronger international cooperation and coordination.

Despite these initial achievements, most participants agree that the strategy no longer reflects current challenges. The document has become outdated and lacks clearly defined objectives, timelines, responsibilities, and an action plan with allocated resources, which limits its effectiveness. In practice, implementation often remains at a declarative level, without binding mechanisms or measurable outcomes.

A lack of political support has been observed, as cybersecurity is not placed among the highest national priorities. There are also institutional fragmentation and insufficient active cooperation towards common goals. Some participants have noted that challenges are not being addressed systematically, primarily because there is no updated national strategy to align the actions of different stakeholders and define shared objectives.

Participants assess the effectiveness of the strategy's implementation in different ways, but no group expresses strong satisfaction with its performance. The private sector, academic institutions, and defence organisations assess the situation somewhat more positively, while public institutions perceive the strategy as least effective, reinforcing the impression of limited operational support within public administration.

Key challenges

- An outdated strategy that no longer reflects the current security environment and emerging threats.
- Unclear division of responsibilities and a lack of coordination among stakeholders.
- Limited financial and human resources that hinder the implementation of measures.
- Unsystematic approach to addressing challenges in areas such as the development, recruitment and retention of experts, research and development programmes, effective cooperation between the state, research institutions and industry, the development of dual-use technologies, and the improvement of security information exchange, among others.
- Insufficient political support and lack of strategic alignment with other national priorities.
- Low visibility of the strategy among stakeholders and the wider professional community.

Opportunities and recommendations

Participants in the study agree that the continued development of the field requires the updating and modernisation of the national strategy. The new version should include measurable objectives, clearly defined responsibilities, the involvement of all key stakeholders, and an implementation programme with allocated resources. A particular emphasis should be placed on strengthening political support and raising awareness of the importance of cybersecurity as an integral part of national security—both in times of peace and in the context of hybrid threats or multidomain warfare.

They also stress that Slovenia should maintain its integration within European and Euro-Atlantic structures, while at the same time strengthening internal coordination

mechanisms, especially the role of the Government Information Security Office (URSIV) as the central coordinating authority. Only in this way will it be possible to move from a declarative to a truly operational and well-coordinated implementation of national policy.

3.2 Main stakeholders in the country

Key governmental agencies and organizations responsible for cybersecurity

- The **Government Information Security Office** of the Republic of Slovenia (URSIV) is the national authority for information security, operating as an independent government service. Its primary mission is to increase resilience to cyber threats that can endanger individuals, companies, state authorities and society as a whole. URSIV connects stakeholders in the national information security system and coordinates operational capabilities in the system at a strategic level.
- The **NCC-SI** (National Coordination Centre for Cybersecurity Slovenia) is Slovenia's national hub for coordinating cybersecurity efforts under the EU Cybersecurity Competence Network. It connects public, industry, academic, and civil stakeholders to drive research, innovation, and capacity-building, while facilitating EU funding, advanced technologies, and cross-border cooperation for stronger cyber resilience.
- **SI-CERT** is Slovenia's national cybersecurity incident response team, operating under the ARNES public institute. It serves as the central point for handling cybersecurity threats and incidents affecting the broader Slovenian internet community, including individuals, businesses, and critical infrastructure. SI-CERT focuses on detecting, analysing, and coordinating responses to cyber incidents, while also raising public awareness and promoting cybersecurity best practices at the national level.
- **SIGOV-CERT** is Slovenia's governmental cybersecurity incident response team under URSIV. It safeguards public administration's digital infrastructure by identifying, analysing, and responding to cyber threats, while strengthening network resilience and ensuring secure coordination during incidents.
- **Individual ministries** — such as the Ministry of the Interior, Ministry of Defence, Ministry of Digital Transformation, and others—have their own internal organizational units dedicated to cybersecurity. Notably, several of these ministries also play a broader role by managing funds that support industry development. These include the Ministry of Defence (MORS), the Ministry of Higher Education, Science and Innovation (MVZI), the Ministry of Cohesion and Regional Development (MKRR), the Ministry of Digital Transformation (MDP), and the Ministry of the Economy, Tourism and Sport (MGTS).

- **AKOS** Agency for Communication Networks and Services of the Republic of Slovenia is an independent regulatory authority in Slovenia that oversees electronic communications, postal services, and radio/TV/media broadcasting. It ensures fair competition, manages the radio-frequency spectrum and numbering, supervises network security and service continuity, and enforces user rights in digital service
- **DOVOS** (Defence, Security and Resilience Company) is a state-owned investment company fully owned by the Republic of Slovenia. Its core mission is to support the development and commercialization of defence, security, and resilience technologies in Slovenia by investing in domestic firms and strategic partnerships.
- **Agency for the Promotion of Investment and Entrepreneurship in Dual-Use Technologies** (Agencija za spodbujanje investicij in podjetništva na področju dvojne rabe) under the Ministry of the Economy, Tourism and Sport (MGTŠ) supports investment, development, and commercialization of dual-use technologies by connecting industry, defence, and civil innovation ecosystems within EU frameworks.

Private sector: There is no exact number of companies involved in cybersecurity, as companies also carry out other ICT activities. A smaller proportion of them also cooperate with the Ministry of Defence. Critical infrastructure players are also essential components of Slovenia's cybersecurity ecosystem, as they operate and safeguard the nation's vital systems and services. Their resilience and protection are crucial for maintaining national security, economic stability, and public trust. This group includes key organizations in sectors such as telecommunications, energy, transport, finance, healthcare, and water management, all of which rely on strong cybersecurity measures to ensure uninterrupted operation.

Involvement of the private sector in cybersecurity initiatives

- SeKV (Sekcija za kibernetisko varnost) is the cybersecurity working group within the ICT Association of Slovenia (ZIT) at CCIS. It unites industry, academia, and public sector stakeholders to promote cybersecurity awareness, dialogue, contribute to national policy, and drive collaboration on national and EU cybersecurity initiatives, while supporting skills and standards development in industry.
- GOIS (Gospodarsko interesno združenje – Grozda obrambe in zaščite Slovenije) is an industry cluster and economic interest association linking Slovenian companies, research institutions, and stakeholders in defence, protection, and security. It strengthens innovation, cooperation, and global competitiveness, supporting members in joint projects, EU and NATO initiatives, and strategic partnerships.

Academic and research institutions contributing to cybersecurity innovation, education, and policy development:

- University of Maribor, Faculty of Electrical Engineering and Computer Science is involved in research on network security, software security, and cyber-physical systems. It also supports cybersecurity education.
- University of Ljubljana, Faculty of Computer and Information Science,
- University of Ljubljana, Faculty of Electrical Engineering,
- University of Ljubljana, Faculty of Social Science,
- Gea college,
- Jožef Štefan Institute conducts research in areas related to cybersecurity, including cryptography, artificial intelligence, and secure systems. Participates in national and European cybersecurity projects.
- Slovenian National Building and Civil Engineering Institute (ZAG) works on the resilience and protection of critical infrastructure, including aspects of cyber-physical system security in the context of infrastructure protection.
- Institute for Corporative Security Studies (ICS-Ljubljana) engages in research and training related to cybersecurity, critical infrastructure protection, and hybrid threats. Participates in national and international security cooperation.

NGO – Civil society:

- Women4Cyber Slovenia is the national chapter under the umbrella of the European foundation. It organizes events, promotes education and professional development, and advocates for gender diversity in Slovenia's cybersecurity sector.
- Zavod Vsak is a Slovenian NGO that promotes digital literacy, safe internet use, and youth empowerment. It educates children, parents, and teachers on online safety, cyberbullying prevention, and digital citizenship through workshops, campaigns, and educational materials.
- Danes je nov dan (Today is a New Day) is a Slovenian NGO focused on digital rights, civic tech, and democratic participation. It develops open-source tools, promotes transparency, and advocates for privacy, digital security, and responsible tech use through campaigns and community projects.
- Državljan D (Citizen D) is a Slovenian non-governmental promoting civic engagement, open government, and digital democracy. It advocates transparency, accountability, and citizen participation through digital tools and open data, while addressing privacy, digital rights, and responsible tech use.

Based on the input from all participants, the cybersecurity ecosystem in Slovenia consists of key stakeholders from the public, private, and research sectors. Among the central

institutions, the Government Information Security Office (URSIV) plays a strategic role as the national coordinator, while SI-CERT serves as the operational unit for handling cybersecurity incidents, analytic and cybersecurity awareness for the public. Relevant ministries, responsible for national security, public administration, and internal affairs, also play a significant role by running their Security Operations Center (SOC). Law enforcement agencies and the national defence system are actively involved in the ecosystem as well.

Research organisations and universities make an important contribution by developing knowledge and expert solutions, while the private sector provides cybersecurity services, technologies, and innovations. In recent years, different forms of cooperation have emerged, such as the SeKV cluster, which supports collaboration and knowledge exchange among stakeholders. At the operational level, progress can be seen especially in cooperation during incident response and in joint project implementation, which has contributed to gradually strengthening the national cybersecurity system.

Cooperation between stakeholders does exist; however, there is potential to develop it further by establishing a more systematic and long-term approach. Currently, cooperation is often limited to individual cases or specific projects, while strategic planning, preventive action, and cross-sectoral cooperation could be strengthened further. In addition to the existing weekly coordination among state authorities, coordination at the strategic level should be established to enable the inclusion of industry — both R&D organisations and providers of cybersecurity products and services.

Better definition of responsibilities, clearer cooperation structures, and stronger support for information sharing would enhance trust among stakeholders and strengthen the overall resilience of Slovenia's cyberspace.

3.3 National cybersecurity challenges and gaps

The national cybersecurity landscape faces several structural and operational challenges that hinder the development of a resilient and coordinated defence ecosystem. Slovenia is experiencing significant development gaps in the field of cybersecurity, which affect the resilience of the state, the economy, and the defence system. Although there is a general awareness of the importance of cybersecurity, the development of capabilities, structures, and processes does not yet enable a comprehensive and systematic approach to risk management. Progress is visible mainly in certain areas; however, measures are often uncoordinated and short-term, which limits the overall effectiveness of the system. Challenges arise at the human, organisational, technical, and strategic levels, with these elements mutually reinforcing and deepening one another.

Key challenges

- Lack of experts and competencies: The most prominent gap lies in the shortage of skilled professionals – not only in technical roles but also in leadership and strategic positions. There is a lack of people capable of providing security solutions, managing risk oversight, and leading the development of national capabilities. These challenges are further aggravated by limited opportunities for education and training, the low attractiveness of the profession among young people, and the migration of experts abroad. Slovenia has not yet adopted a systemic approach to workforce development, and a strategy should be prepared to connect academia, industry, and public administration within a common framework for competence development.
- Insufficient funding and low political priority: A frequently highlighted challenge is the lack of stable financial resources and limited political support. Funding is insufficient both for the development of national infrastructure and for investments in research, innovation, and the maintenance of existing systems. Due to limited resources, many institutions operate reactively and without a long-term vision, reducing the effectiveness of measures. Cybersecurity remains subordinate to other national priorities, and as a result, initiatives often remain at the level of declarative commitments without clear implementation programmes and the necessary resources.
- Low awareness and organisational maturity: In many organisations, cybersecurity is still perceived mainly as a technical issue rather than as part of comprehensive risk management. In numerous cases, standardised procedures, regular risk assessments, or business continuity plans are not in place. The lack of awareness also affects the level of investment – a low perception of risk leads to limited interest in protective measures, further increasing the vulnerability of systems.
- Poor coordination and fragmented responsibilities: It has been emphasised that Slovenia lacks effective coordination among institutions, as responsibilities are often dispersed and communication inconsistent. Interdepartmental cooperation takes place mainly on a project basis and in a non-systematic way, without shared strategic leadership. This fragmentation leads to duplication of activities, inefficient use of personnel, and inconsistent allocation of resources, all of which reduce the effectiveness of the national system.
- Technological and structural limitations: At the technical level, challenges are linked to outdated infrastructure, particularly around operational technologies (OT) and legacy systems, many of which are insufficiently protected or no longer maintained. In addition, Slovenia remains highly dependent on foreign technological solutions, which reduces its strategic autonomy and limits the development of domestic expertise.

Opportunities and recommendations

Despite numerous limitations, stakeholders agree that Slovenia has a solid foundation for progress, provided it succeeds in integrating existing capacities into a coherent system. The following key opportunities have been identified:

- Developing a national cybersecurity workforce strategy that will define objectives, incentives, and mechanisms for cooperation among key stakeholders.
- Ensuring stable and targeted funding, particularly for infrastructure, research, innovation, and dual-use technologies.
- Establishing systematic coordination between government bodies, industry, and the research community, with clearly defined responsibilities and decision-making processes.
- Develop a cybersecurity culture through continuous awareness campaigns, encouraging appropriate daily practices from the individual to management level.
- Encouraging the development of domestic technological solutions and reducing dependence on foreign providers.
- Promoting international cooperation of Slovenian experts and organisations within European and Euro-Atlantic networks, exercises, and research consortia.

Through greater national alignment, investment in knowledge, and the development of domestic solutions, Slovenia could strengthen the resilience of its cyberspace and reduce reliance on foreign technologies.

3.4 International cooperation and partnerships in cybersecurity research

Slovenia participates and collaborates through different activities like:

- Participation in international cybersecurity frameworks and organisations that support cybersecurity research, policy alignment, and capacity development. At the European level, Slovenian stakeholders are engaged with the European Union Agency for Cybersecurity (ENISA) and the European Cyber Security Organisation (ECSO). These collaborations include involvement in EU-wide working groups, good practice sharing, and access to research platforms.
 - Slovenian organisations have been partners in EU-funded pilot projects focusing on competence building.
 - Through the **European Digital Innovation Hub Slovenia (EDIH Slovenia) – part of the EU's EDIH network**, Slovenian actors also take part in activities

that support the adoption of cybersecurity technologies by small and medium-sized enterprises and public organisations.

- In addition, Slovenia relates to initiatives such as **Women4Cyber Slovenia**, the national chapter of the Women4Cyber Foundation, which promotes training and inclusion in cybersecurity education and employment.
- Defence-oriented cooperation
 - Through its participation in **EDA CapTech Cyber** (European Defence Agency (EDA), 2025), Slovenia contributes to research and development in the field of cyber defence, transferring results to the national industry and helping to build national defence capabilities.
 - Slovenian teams have also participated in **Locked Shields**, an annual cyber defence exercise organised by the **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)**. This exercise is used to test and improve technical, operational, and decision-making processes during large-scale simulated cyber incidents.
- Research and capacity-building platforms
 - Slovenia is included in EU cybersecurity research and training infrastructures such as **CyberHubs**, which offer environments for cyber range testing, education, and skills development.
 - In the context of the **COcyber project**, Slovenian partners contribute to joint activities that aim to align civilian and defence cybersecurity efforts. These include work on dual-use technology, information-sharing practices, and collaborative response models for cross-sector incidents.
 - Slovenian experts have also taken part in the **Cybersecurity Atlas** (European Commission, 2025) maintained by the European Commission, which connects research institutions working on cybersecurity topics across Europe.
 - Slovenian companies regularly apply for and receive funding through European calls related to cybersecurity research and development. These efforts are supported through programmes such as the European Defence Fund (EDF), Cat-B CapTech Cyber projects, Horizon Europe, and NATO's innovation initiatives. Many of the resulting consortia are formed through SeKV, the national cybersecurity industry network, by fostering collaboration among companies, research institutions, and public stakeholders.
- Information-Sharing and Joint Exercises
 - URSIV is the national authority and single point of contact; operationally, SI-CERT (national CSIRT) and SIGOV-CERT (government CSIRT) handle cooperation. The roles, incident reporting, and collaboration are defined in

the ZInfV (Republic of Slovenia, 2018) / ZInfV-1 law (Republic of Slovenia, 2025) (NIS2 transposition).

- The INTERCEPT project is building a cross-border MISP platform for threat intelligence sharing (TLP, IoCs, etc.) with Slovenian participation; the goal is standardized, automated CTI exchange between partners.
- Operational guidance and practice. SI-CERT publishes annual reports, participates in EU programs (e.g., Cyber Balkans), and coordinates awareness campaigns such as “Safe on the Internet”; these include guidelines for incident reporting and information sharing.
- ENISA Cyber Europe 2024: Slovenia fielded 18 teams; the after-action report (European Union Agency for Cybersecurity (ENISA), 2024) highlights gaps and recommendations for resilience across the EU.
- Adriatic Regional Cyber Cooperation Exercise ARSC2EX 24 (2024): Slovenia hosted this multinational exercise in Postojna (June–July 2024, with regional states + US); the focus was cross-border cooperation and response procedures.
- NATO cyber exercises Locked Shields. Slovenia regularly participates in NATO’s largest annual cyber defence exercise, designed to strengthen intersectoral response capabilities. National team has participation from defence and industry.
- Slovenian institutions participate in information-sharing activities organised by ENISA and other EU bodies, including the use of ISAC (Information Sharing and Analysis Centre) toolkits and participation in **Cyber Europe** exercises.

The **COcyber project** further highlights Slovenia’s involvement in structured needs assessment and joint roadmap development for cross-sector cooperation.

International Engagement: Slovenia takes part in European and Euro-Atlantic cybersecurity structures and expert networks. Stakeholders participate in the activities of national and sectoral CSIRTs, cooperate with European agencies and associations, maintain bilateral relations, and take part in research, development, and operational projects. Slovenia is also involved in initiatives for the exchange of threat information (e.g. SOC networks), international exercises, and capacity-building programmes.

Benefits: The most frequently mentioned benefits include access to international knowledge and good practices, faster transfer of experience to the national environment, opportunities for research, development and innovation (RDI) and human resource development, as well as better alignment with European standards. International cooperation increases the visibility of national experts, facilitates entry into foreign markets, supports networking, and helps build national cybersecurity capacities (for example through joint projects, co-financing or threat intelligence exchange). Interviewees

also noted that international cooperation often encourages stronger cooperation among domestic stakeholders.

Challenges: Commonly reported challenges include limited resources to systematically take advantage of international opportunities and the lack of a long-term strategy that is consistently implemented in practice. Information from international events is transmitted to national stakeholders rather slowly, as the volume of information is extensive. Stakeholder fragmentation is also seen as an obstacle. There are capacity and staffing limitations (both in applying for calls and in project implementation), uneven quality of partnerships, slow administrative procedures in some programmes, and insufficient level of project results implementation in operations

Examples of cooperation and programmes: Examples of recognised good practices and cooperation arrangements include:

- participation of the defence and industry joint team in the international cyber exercise Locked Shields (planning, joint training, team coordination),
- cooperation in SOC networks and agreements for threat information exchange (including through providers and open-source platforms),
- involvement in European and Euro-Atlantic initiatives (e.g. ENISA, ECSO, European CSIRT and crisis networks, NCC/ECC, ransomware initiatives),
- bilateral partnerships and cooperation agreements that enable access to shared capacities and crisis support,
- RDI projects and capacity-building programmes (training, involvement of higher education, cooperation between research and industry partners).

The overall impression is that international cooperation brings clear benefits in terms of knowledge, capabilities, and alignment with standards. However, its impact could be further increased through stronger strategic direction, better use of results in practice, and improved human resources and coordination.

4 Technology transfer framework

This section explores mechanisms through which cybersecurity technologies are transferred within and between different sectors, including civilian and defence industries. It assesses existing technology transfer policies, identifies best practices, and highlights challenges faced in facilitating smooth innovation generation and transfer.

4.1 Definition and importance of technology transfer in cybersecurity

Technology transfer in cybersecurity refers to the process of sharing or moving cybersecurity related technologies, knowledge, methodologies, practices or tools from one organization or sector to another to improve cyber defence capabilities. The main identified mechanisms are cooperation in the field of research and development, licences transfer and, less frequently, spin-offs and start-ups.

Effective technology transfer is particularly important in contexts where resources are limited. By enabling the adoption of proven solutions from one environment to another, it reduces duplication of effort, accelerates innovation uptake, and builds resilience across sectors. In the global context, this also includes the transfer of technologies and expertise from developed to developing countries, not only to support economic growth but also to raise the overall level of cyber resilience internationally.

“Research transforms money into knowledge; technology transfer in cybersecurity transforms knowledge into protection, resilience, and innovation.”

Technology transfer includes intellectual property management, business modelling, and support for commercialisation, serving as a bridge between innovation and implementation.

Technology transfer enables organisations faster access to expertise, fosters competence development, and strengthens domestic capacities. For the state, it contributes to innovation, competitiveness, and national security, while reducing dependence on foreign solutions and supporting the development of niche technologies applicable in both civilian and defence domains.

Despite its importance, technology transfer in Slovenia remains fragmented and underdeveloped. The gap between research and market application is wide, and cybersecurity-related technology transfer is not yet recognised as a national priority. Universities often remain isolated from industry, collaboration is sporadic, and the system lacks sufficient human and financial resources as well as a coherent long-term strategy.

Key challenges

The absence of a coherent long-term vision and strategy with properly structured program limits the ability of Slovenia to position itself within European defence-innovation programmes and to coordinate better its participation in EU funding schemes for

cybersecurity and dual-use R&D. This challenge is further compounded by the lack of a clear national strategy to guide research priorities and knowledge transfer, which would be essential for ensuring alignment between academic research, industrial needs, and national strategic objectives. It has resulted in fragmented efforts, research outcomes are rarely transformed into marketable products, as there are few incentives for commercialisation and limited support for partnerships.

Universities are frequently closed for cooperation, while companies are fragmented, often foreign-owned, and primarily driven by short-term profit rather than longer term strategies and leaded by national technological development objectives. The role of the state remains unclear: while it finances public research institutions, it does not provide guidance on priority technologies or long-term development programmes.

Exchange of information on research topics, planned research projects, which would encourage the involvement of companies, research organizations and state bodies are rarer than the rule. Project ideas most often begin with the publication of a call for proposals, which reduces the innovativeness of solutions and the final success of the project. With changing threats and market demands, companies are increasingly aware of the necessity of involvement in R&D projects, but they are most often undernourished with knowledge and human resources.

As a result, Slovenia continues to depend heavily on foreign technologies, losing both domestic expertise and talent to international markets.

Opportunities and recommendations

To improve technology transfer and increase the impact of research on cybersecurity innovation, Slovenia should strengthen coordination and establish clearer strategic direction. Key opportunities and recommended actions include removing obstacles and incentives for implementation at operational levels.

A coordinated, innovation-driven approach would allow Slovenia to transform research achievements into practical value, enhance national cybersecurity maturity, and strengthen its position within the European innovation ecosystem.

4.2 Legal and regulatory framework governing technology transfer research

Technology transfer in Slovenia is supported by a set of interlinked laws, policies, and strategies that define how research results can be protected, commercialized, and shared with industry and society. The most relevant instruments include:

- Law on Scientific Research and Innovation Activities (ZZrID) (Republic of Slovenia, 2021) provides the legal foundation for cooperation between research organizations and industry, including the ability for public research institutions to establish spin-offs. It explicitly requires internal rules for commercialization (pricing, sale of services, cooperation contracts). By structuring how publicly funded research can move into the market, it is the backbone of technology transfer in Slovenia.
- Higher Education Act (ZViS) (Republic of Slovenia, 1993) defines the mission of universities to include not only education and research but also active collaboration with industry and society. It provides the legal basis for universities to establish companies, incubators, and technology transfer offices (TTO) that channel research results into practice. In addition, it allows institutions to set internal rules on intellectual property management, enabling clear frameworks for licensing and commercialization.
- Industrial Property Act (ZIL-1) (Republic of Slovenia, 2001) governs patents, trademarks, designs, and related rights, which are the primary vehicles of technology transfer. Licensing and assignment rules allow research outputs to be transferred to companies or investors under clear legal procedures. Without this act, research institutions would lack the legal means to commercialize inventions or protect their value.
- Copyright and Open Access Regulations (Republic of Slovenia, 1995): Slovenian rules mandate open access for publicly co-funded research publications, with exceptions for intellectual property (IP), personal data, or national security. This ensures that knowledge generated with public funds can be widely disseminated while still protecting valuable results through IP mechanisms. The balance between openness and protection is crucial for effective technology transfer.
- Resolution on the Slovenian Scientific Research and Innovation Strategy 2030 (ZRISS 2030) (Government of the Republic of Slovenia, 2023b): this strategic document defines national priorities for research, innovation, and technology transfer until 2030. It emphasizes the need for stronger collaboration between government, academia, and industry, and for aligning transfer activities with digital

transformation and sustainability goals. It guides how institutions design and fund technology transfer mechanisms in practice.

- National Intellectual Property Strategy 2030 (Government of the Republic of Slovenia, 2024): the document sets long-term goals for strengthening IP awareness, use, and enforcement in both the public and private sector. It promotes the integration of IP into research and innovation ecosystems, making technology transfer more systematic. By prioritizing capacity building and awareness, it reduces barriers for SMEs and researchers engaging in commercialization.
- Digital Slovenia 2030 (Government of the Republic of Slovenia, 2023a) is the umbrella plan for Slovenia's digital transformation until 2030, aligning with EU ambitions and developed through broad stakeholder consultation. It places individuals and their environment at its centre, and proposes measurable goals across infrastructure, digital skills, economy, public services and cybersecurity. It further mandates a strategic council and inter-ministerial group to coordinate implementation, with funding via national and EU sources but no direct financial commitments in the document itself.

Supporting acts are:

- The Programme of Collaborative R&D Projects and Other Projects Subject to State Aid 2022-2030 (Program sodelovalnih raziskovalno-razvojnih projektov in drugih projektov, ki so predmet državnih pomoči Ministrstva za visoko šolstvo, znanost in inovacije 2022-2030) (Ministry of Higher Education, 2022) sets out the framework by which the Ministry of Higher Education, Science and Innovation will allocate public support for research, development and innovation (RDI) through the period 2022-2030, aligning with key national and EU strategic documents. It emphasises strategic priorities and establishes clear principles, legal bases and indicators to guide the state-aid measures.
- Companies Act (ZGD-1) (Republic of Slovenia, 2006) provides the legal framework for establishing companies, including spin-offs from research institutions that are essential vehicles for technology transfer. It enables universities and public research organizations to hold equity in such companies, thereby moving innovations from the public sector into the market. In addition, it regulates corporate governance and contractual relations that underpin licensing, joint ventures, and other forms of commercialization.
- Public Procurement Act (ZJN-3) (Republic of Slovenia, 2015) supports technology transfer indirectly by enabling mechanisms such as innovation partnerships and dedicated procedures for research and development contracts. Through these instruments, public authorities can act as early adopters of new technologies, helping innovations move from research to the market. The Act also opens

opportunities for SMEs and start-ups, which are often key drivers of commercialization and applied research.

In Slovenia, the legal and institutional framework for technology transfer is partially established and draws on several sources. The foundation is set by the Research and Innovation Act, which introduced knowledge transfer offices and encourages cooperation between research organisations and the private sector. Additional elements come from EU legislation and directives, as well as defence and export control regimes that regulate dual-use technologies. Accreditation and certification systems further support the transfer of technologies and participation in international programmes.

However, the framework is often perceived as complex, fragmented, and difficult to navigate, since different areas are regulated in separate documents.

In practice, the system is hindered by administrative burdens, inconsistent guidelines across ministries, and unclear rules on intellectual property and dual-use technologies. The well-known “valley of death” between Technology Readiness Levels (TRL) 4 and 7 remains a major obstacle, where many promising projects fail to reach operational application. Challenges often arise concerning the rights to use the results of R&D national or EU projects in operational practice, or simply due to inadequate dissemination of results that could support their transition into practical application.

Project-based funding is limited and often short-term, which makes long-term planning and development difficult. Although Slovenia benefits from mechanisms such as university consortia and innovation alliances, and participates in EU and NATO programmes (EDF, Horizon Europe, EDA), the national framework still lacks coherence. Knowledge transfer offices exist, but they are not yet widely recognised or influential, and research institutions remain oriented towards academic outputs rather than practical application.

Participation in international programmes and certification schemes also helps exchange knowledge and build capacity. There is growing awareness that technology transfer benefits both sectors and contributes to European security and competitiveness.

In recent years, the Ministry of Defence, based on its internal regulations, has been actively encouraging industry to participate in national and European R&D projects — from fundamental studies of specific fields to higher TRL levels and preparations for operational use.

Key challenges

The regulatory environment remains fragmented and overly bureaucratic, slowing the pace of technology transfer and project implementation. The system’s complexity and

loose coordination between ministries create uncertainty and discourage cross-sector cooperation. Research activities are rarely aligned with operational needs, and the existing legislation does not sufficiently encourage the practical application of research results. The Digital Slovenia 2030 (Government of the Republic of Slovenia, 2023a) umbrella strategy, in the Cybersecurity chapter, does not identify the areas of technology transfer or research and development as necessary work to strengthen resilience among its implementation objectives. Knowledge transfer offices exist but are not well known or influential, and researchers are still mostly rewarded for academic publications, not for successful transfer of technology. Dependence on foreign solutions – licences agreements and the loss of domestic talent abroad further weaken national innovation capacity.

Companies often lack clarity on national priorities, while universities remain relatively closed and disconnected from industrial needs. There is no clear coordinating institution linking the state, research organisations, and the private sector. The absence of a national strategy for cybersecurity-related R&D and dual-use technologies further limits progress.

Regulations concerning classified information, dual-use technologies, and engagement of civilian experts in defence-related projects are well established but can be administratively demanding, particularly for SMEs and universities. Procedures within national funding and innovation frameworks (such as ARRS/ARIS and SPIRIT) are often perceived as rigid and overly formal, which can complicate project participation and slow implementation. The unclear legal framework for civilian participation and the complex rules governing dual-use technologies often discourage smaller organisations from involvement. Rules on dual-use and classified information discourage smaller companies and universities from entering defence-related R&D, as compliance procedures are complex and resources demanding.

Opportunities and recommendations

Strengthening the legal and institutional framework requires clearer priorities, better coordination, and practical mechanisms that promote cooperation and implementation. Key opportunities and recommendations include:

- Develop clear and operational national strategy for technology transfer and cybersecurity and dual-use R&D, that links academia, industry, and defence. The strategy should define measurable objectives, identify priority technologies and funding mechanisms and set national priorities to ensure efficient resource allocation, coordinated innovation efforts and long-term support for research and innovation.

- Establishing a coherent national cooperation framework connecting government, academia, and industry, with clearly defined roles and communication channels.
- Provide clear legal and procedural frameworks for the inclusion of civilian experts in national and defence-related projects and simplify administrative procedures while ensuring transparency in project evaluation and funding allocation.
- Simplify and harmonise legal and administrative procedures governing dual-use technologies and civilian participation in defence-related projects, while providing clearer guidance and practical support for potential participants. These measures would reduce the administrative burden on SMEs and research institutions and promote broader, more effective cross-sector collaboration.
- Expanding a shared national platform and information exchange for collaboration and integration of existing technologies, enabling synergy between public and private initiatives.
- To improve access to the research result, simplifying the transfer of research results to industry, including support for certification and commercialisation of cybersecurity solutions.
- Building domestic capacity and reducing reliance on foreign solutions by investing in national competences, standards, and infrastructure, and supporting the development of local software and hardware for crisis communication and resilience.
- Increasing transparency and providing consistent guidance on intellectual property, certification, and export control to encourage commercialisation and cross-sector collaboration.

A well-coordinated, transparent, and innovation-oriented regulatory framework would allow Slovenia to transform research outputs into practical value, strengthen national cybersecurity capacities, and enhance participation in international research and development programmes.

4.3 National institutions responsible for facilitating technology transfer

Technology transfer in Slovenia is supported by a diverse ecosystem of national authorities, research organizations, and intermediary institutions. These actors provide the legal, financial, and organizational frameworks that enable research results to move from universities and laboratories by companies into the market. The following table outlines the key institutions and initiatives, together with their specific roles in facilitating technology transfer.

Institution / Actor	Role in technology transfer
Ministry of Higher Education, Science and Innovation (MVZI)	Sets national research and innovation policy, oversees ZZrID (Republic of Slovenia, 2021) and ZRISS 2030 (Government of the Republic of Slovenia, 2023b), provides funding instruments and regulatory frameworks for TTO.
Slovenian Research and Innovation Agency (ARIS)	Funds research projects and programmes; integrates knowledge valorisation and TT requirements into funding schemes.
Ministry of Defence (Research, Development and Procurement Sector within the Directorate for Logistics)	Actively engages with European organisations such as the EDA and NATO
Slovenian Intellectual Property Office (URSIL)	Grants patents and IP rights; provides guidance on IP protection and commercialization; aligns Slovenia with EU and international IP frameworks.
Public Research Organisations & Universities	Operate Technology Transfer Offices (TTOs), incubators, and innovation offices; manage patents, licensing, spin-offs, and collaboration with industry.
Technology Parks	Provide infrastructure, mentoring, and networking for start-ups and spin-offs; serve as bridges between research and entrepreneurship.
Slovenian Innovation Hub	National platform connecting academia, industry, and government; facilitates TT projects in health, biotech, ICT, and manufacturing.
Slovene Enterprise Fund (SPS)	Provides grants, seed funding, and venture capital co-financing to innovative start-ups and SMEs for commercialization.

SPIRIT Slovenia	Promotes entrepreneurship and internationalization; supports TT through investment incentives, export promotion, and innovation support schemes.
SRIPs (Strategic Research and Innovation Partnerships)	Thematic clusters (e.g., Smart Cities, GoDigital, Factories of the Future) that link academia and industry in priority areas; key facilitators of collaborative research and TT.
Competence Centres	Public–private partnerships focusing on specific technology fields; support joint R&D and transfer of advanced technologies into industry.
Accelerators	Provide start-ups with mentoring, investment readiness, access to venture capital, and networking; speed up commercialization of innovations.
Regional Development Agencies	Implement regional projects for balanced development; support innovation ecosystems and TT at the regional level, often in coordination with EU funds

Table 4: National institutions responsible for facilitating technology transfer

Technology transfer in Slovenia involves a network of state institutions, research organisations, universities, intermediary bodies, and companies. The main actors include government ministries and agencies (such as the Ministry of Defence), research organisations and universities, as well as intermediary institutions such as ARIS, SPIRIT, SRIPs, competence centres, Innovation Hubs and the Chamber of Commerce and Industry of Slovenia (CCIS). Cooperation among these actors takes place through projects, consortia, and technology transfer offices, yet remains uneven and often dependent on personal networks.

Technology transfer offices (TTOs) are an important part of the institutional structure, but they are often perceived as passive, lacking visibility and a proactive approach in connecting research institutions with industry. Their role in facilitating the commercialisation of research results is limited, and they frequently operate within bureaucratic constraints. There is a clear need for a more strategic, coordinated, and well-resourced approach that defines responsibilities, supports early engagement of industry, and ensures that the private sector – especially small and medium-sized enterprises – becomes more involved in research and development from the outset.

Institutions such as ARIS and SPIRIT play key roles in funding and supporting research, innovation, and entrepreneurship. However, the procedures are often seen as rigid and calls for proposals tend to be directed primarily towards research organisations rather

than fostering strong public–private collaboration. Mechanisms such as SRIPs, competence centres, innovation hubs and clusters offer a foundation for collaboration but are often understaffed and limited in impact. CCIS, through its associations and events, remains an important facilitator of networking and the creation of new project ideas, especially between industry and research institutions.

Key challenges

The institutional framework for technology transfer is weakened by fragmented responsibilities, administrative rigidity, and insufficient coordination between key actors, which can result in overlapping mandates and fragmented communication. Cooperation between civil, defence, academic, and industrial stakeholders often develops within the framework of short-term projects, and systematic mechanisms for long-term coordination are still evolving. Technology transfer offices lack stable funding and are rarely seen as active intermediaries. Research institutions, although publicly financed, are often viewed by companies as bureaucratic rather than supportive partners in innovation.

The absence of a clear national mechanism defining the roles and responsibilities of intermediary organisations limits their effectiveness. Funding for consortia and coordination structures remains unstable, which hinders continuity and the establishment of trust between partners. There is also a lack of systematic inclusion of industry, particularly SMEs, in the early stages of research and development. This results in low commercialisation rates and insufficient alignment between research outcomes and market needs.

Opportunities and recommendations

A more coherent and collaborative framework could significantly enhance the efficiency and impact of technology transfer in Slovenia. To achieve this, the following measures are recommended:

- Simplify administrative procedures and reduce bureaucratic barriers within funding and coordination mechanisms.
- Introduce a clear framework that defines the roles, responsibilities, and accountability of TTOs and intermediary institutions between the state, research organisations, and industry.
- Establish stable and predictable funding for technology transfer offices, clusters, consortia, and intermediary institutions to ensure continuity and professional capacity to support process of innovation with more participants.

- Strengthen the role of incentive organizations (Innovation Hubs, Clusters, Competence Centres), especially in the early stages of the innovation process from the idea to the establishment of a project organization.
- Enhancing the role and visibility of intermediary institutions, such as knowledge transfer offices and technology hubs, to act as facilitators between researchers and end-users.
- Create a national “one-stop shop” platform providing guidance and comprehensive support to companies, particularly SMEs, for engaging in research, innovation, and technology transfer.
- Strengthen collaboration between companies, research institutions, and clusters by promoting joint initiatives and cross-sector consortia focused on practical applications.

A coordinated and transparent institutional approach would enable Slovenia to better connect its research potential with the needs of industry and national security, stimulate innovation, and strengthen the country’s capacity to participate in European and international research and development programmes.

4.4 Incentives and barriers to technology transfer

Slovenian cybersecurity ecosystem contains several emerging enablers and incentive mechanisms that support technology transfer, including dual-use innovation.

These enablers reflect both formal policy instruments and informal cooperation practices that have developed through shared projects, training, and gradual alignment with European frameworks:

- **Governance and coordination enablers:** At the systemic level, the Resolution on Scientific Research and Innovation Strategy 2030 (ZRISS 2030) (Government of the Republic of Slovenia, 2023b) provides the strategic foundation for cooperation between science, industry, and public administration. It explicitly promotes knowledge valorisation and the integration of research into economic and societal processes. The detailed implementation of the strategy is defined by the program of collaborative research and development projects and other projects (Ministry of Higher Education, 2022) that are subject to state aid from the Ministry of Higher Education, Science and Innovation. This policy direction is reinforced by the SRIP GoDigital partnership, which functions as the main horizontal innovation network connecting ICT, cybersecurity, and digital-infrastructure actors. Through joint R&D and project facilitation, SRIP GoDigital creates a structured interface for collaboration and international visibility. The National Cybersecurity Coordination

Centre (NCC-SI) also represents an important institutional step toward linking Slovenian cybersecurity R&D with the EU programmes.

- **Legal and policy support:** Legal reforms have established clearer conditions for knowledge transfer and commercialisation. The Law on Scientific Research and Innovation Activities (ZZrID) (Republic of Slovenia, 2021) grants research organisations autonomy to commercialise results, establish spin-off companies, and license intellectual property to external partners. Moreover, the ongoing alignment of national regulations with EU directives, notably NIS-2 (European Union, 2022a) and the European Defence Fund framework (European Union, 2021b), enhances compatibility of Slovenian cybersecurity governance with European standards.
- **Financial and innovation instruments:** A broad set of national and European financial mechanisms supports applied research and technology demonstration. Funding agencies such as ARIS, SPIRIT Slovenia, and the Slovene Enterprise Fund provide co-financing for innovation, while EU programmes including Horizon Europe, Digital Europe, and the European Defence Fund enable dual-use projects and international collaboration. In addition, innovation vouchers, tax incentives, and SME support schemes help reduce the cost of participation in R&D partnerships.
- **Human capital and skills development:** Human-resource development is a central enabler of technology transfer. Programmes such as CyberHubs and AI4SI expand the national pool of cybersecurity and digital specialists, providing opportunities for training in advanced technologies and cross-domain applications. Several universities have introduced or updated courses in cybersecurity engineering and digital forensics, while research institutions and companies increasingly cooperate on joint training, internships, and certification schemes.
- **Trust and collaboration mechanisms:** Beyond formal policy frameworks, trust-building activities are emerging as effective enablers of cooperation. Joint simulation exercises such as Locked Shields have strengthened professional relationships and interoperability among military, academic, and industry teams. Cluster networks, professional associations, and SRIP platforms provide neutral venues for dialogue and project matchmaking, while interpersonal and informal networks remain a powerful medium for knowledge exchange across institutional boundaries.
- **Cultural and strategic drivers:** Finally, the cultural context is gradually shifting in favour of innovation. This trend is reinforced by Slovenia's strategic alignment with European digital and defence agendas, which enhances credibility and provides access to transnational initiatives within the European Research Area and Digital Europe programmes.

Technology transfer in the field of cybersecurity in Slovenia is shaped by institutional, legal, financial, and cultural factors. The ecosystem is gradually developing through participation in European and international initiatives, although it still relies largely on project-based cooperation rather than fully established systemic frameworks. Positive progress can be observed through participation in EU and NATO research programmes, consortia supported by the Ministry of Defence, and growing collaboration between academia, industry, and public institutions. However, several structural and procedural challenges continue to influence the pace and effectiveness of technology transfer, particularly in bridging the gap between research results and practical application.

Key barriers and incentives

- **Human capital and knowledge retention** remains a critical factor.
 - The shortage of qualified cybersecurity professionals remains a major obstacle, particularly for dual-use and defence-related activities.
 - Both public and private institutions face difficulties in attracting and retaining experts, while many professionals continue to move abroad.
 - Education and training programmes are still largely specialised by discipline; encouraging a more multidisciplinary approach would better align skills with market and national needs.
 - Participation in European consortia provides valuable incentives for knowledge exchange, professional mobility, and access to advanced expertise.
- **Financial and commercialisation mechanisms:**
 - Public funding mainly supports early-stage research, with limited instruments for advancing technologies to higher readiness levels or for validation and certification.
 - This creates a persistent “valley of death” between research outcomes and operational or market use, especially for smaller organisations lacking dedicated resources.
 - Weak public–private partnerships further constrain investment continuity and reduce the opportunities for joint development of solutions that could bridge research and industry needs.
 - Expanding follow-up schemes or intermediary mechanisms for technology maturation could strengthen the innovation chain and improve the sustainability of R&D outcomes.
- **Trust, culture and cooperation:**
 - Awareness of cybersecurity’s importance is increasing, yet collaboration between government, academia, and industry remains uneven.

- Limited trust and inconsistent information exchange continue to hinder effective cooperation, although repeated joint exercises and partnerships are helping to build a more open, knowledge-driven culture.
- **Positive incentives and opportunities:**
 - Participation in EU and NATO frameworks such as EDF, Horizon Europe, and EDA provides access to funding, expertise, and international networks.
 - Cross-sector exercises and research collaborations improve mutual understanding and operational interoperability.
 - Regulatory alignment with EU standards facilitates international cooperation and enhances transparency.
 - Growing recognition of cybersecurity as both a strategic priority and a business opportunity encourages organisations to invest in joint innovation and development.

Opportunities and recommendations

Building on existing achievements and addressing the remaining challenges will help Slovenia further strengthen its technology transfer ecosystem. The following measures could support this process:

- A strategic body to promote cooperation between companies, R&D organisations, and the government, and to develop a research and development programme in cybersecurity, including aspects of dual-use technologies.
- Introduce additional instruments for the commercialisation of research results, such as intermediary support and spin-out incentives.
- Recognise and reward successful technology transfer and commercialisation outcomes as integral components of research evaluation frameworks.
- Promote cooperation between research institutions and companies through targeted funding, tax incentives, and programmes that foster applied research.
- Encourage early participation of industry, including SMEs, in research and innovation initiatives to ensure practical applicability, technology uptake, and long-term impact.
- Encourage a stronger multidisciplinary rather than purely interdisciplinary approach to education would enhance collaboration, foster innovation, and better align educational outcomes with the evolving needs of industry and society. Strengthen education and training programmes that integrate dual-use and cybersecurity components to build a skilled and adaptable workforce.

A balanced combination of strategic coordination, supportive policy instruments, and a culture of partnership will enable Slovenia to enhance the efficiency of its technology

transfer processes, increase national resilience, and reinforce its position within the broader European research and innovation landscape.

4.5 Examples of successful technology transfer initiatives

This chapter highlights concrete examples of technology transfer initiatives that demonstrate how research and innovation projects create impact.

The analysis of projects related to cybersecurity, involving R&D organizations and end-users, focused on risk assessment, vulnerabilities, and mitigation measures with various emphases, including IoT, cloud services, critical infrastructure, and the use of existing tools.

The analysis also highlighted the categorization of equipment used for both offensive and defensive purposes. This does not refer to dual use in the sense of civilian or military application.

All project results with the participation of national stakeholders are also valuable for the field of military defence. However, there is no indication that these results have been presented to the defence sector.

Horizon Europe projects in the field of cybersecurity in the period 2022–2025.

Project ID	Project acronym	Comment	Participants
HE-101075714	R2D2	A comprehensive cybersecurity approach in the field of electricity	ELPROS D.O.O. Elektro Ljubljana, d.d. EL OVE
HE-101095542	CYLCOMED	Implementation of the use of tools for detection and prevention in the field of medical equipment.	XLAB d.o.o.
HE-101073909	ATLANTIS	Vulnerability assessment and penetration testing	TELEKOM SLOVENIJE Snep DARS SZ DOO

			SZ IN PETROL DD LJUBLJANA INSTITUTE FOR CORPORATIVE SECURITY STUDIES LJUBLJANA JSI MINISTRY OF INFRASTRUCTURE URSIV
HE-101070537	CROSSCON	Detection in the field of IoT	Beyond Semiconductor
HE-101168438	INTACT	AI, cloud , IoT	Beyond Semiconductor
HE-101093274	TrustChain	internet	UNIVERZA V LJUBLJANI
HE-101093126	ACES	Cloud security	UNIVERZA V LJUBLJANI

Table 5: Horizon Europe projects in the field of cybersecurity in the period 2022–2025

Seven cybersecurity service providers and seven service users from Slovenia are involved. The outcomes of all projects, both completed and ongoing, are applicable and transferable to the defence sector.

Additional projects are:

- CyberSEAS – CyberSEAS (Cyber Securing Energy dAta Services) is an EU-funded project that enhances the cybersecurity and resilience of European energy systems and supply chains. Participants: SI.CERT; ICS; Eles, Petrol
- CapTech Cyber projects are defense-focused initiatives that also strengthen the capabilities of participating organizations for civilian applications.
 - PASEI II
 - REMUDO Participants: CreaPlus, University of Maribor and University of Ljubljana
 - BRICO TBB 5 A03: Building trust and cyber resilient military CIS using untrusted components. Participants: CreaPlus, University of Maribor and University of Ljubljana
 - SPARTA-2 – initial phase
- Nacional CRP projects:
 - 2023Cyber Cyber risk analysis

Although the number of recognised technology transfer cases in cybersecurity in Slovenia remains limited, several positive examples demonstrate how collaboration between

research institutions, industry, and state organizations can yield tangible operational results. Successful initiatives typically involve clearly defined objectives, motivated and competent teams, early involvement of end-users, and strong coordination between partners.

Examples of good practice include participation in the Locked Shields cyber defence exercise, where coordinated planning, joint training, and team synchronisation proved key to effective collaboration between civilian and defence sectors. Cooperation within Security Operations Centre (SOC) networks and threat intelligence sharing frameworks also represents a form of knowledge and technology transfer that strengthens collective cybersecurity capability.

Additional examples can be found in selected EU and RDI projects focused on critical infrastructure protection, artificial intelligence in defence, and the development or piloting of national cyber range capabilities. The Cybersecurity Academy is another recognised case of applied knowledge transfer.

These examples demonstrate that well-managed cooperation, supported by stable funding and a strategic focus, can significantly accelerate the transition from research to practice and enhance national cybersecurity resilience.

5 Information sharing mechanisms

As cybersecurity is a systemic domain, no single organisation can manage all threats on its own. Effective defence against rapidly evolving threats depends not only on the technical capabilities of individual organizations but also on their willingness and ability to exchange knowledge, experiences, and actionable intelligence. By fostering timely collaboration between public institutions, private industry, and academia, information sharing helps build collective resilience and ensures that no single stakeholder has to face complex cyber challenges in isolation.

This section examines how cybersecurity-related knowledge, threat intelligence, and best practices are shared between national and international stakeholders. It evaluates the effectiveness of current information-sharing platforms and highlights areas where improvements are needed.

5.1 Existing national cybersecurity information-sharing policies and frameworks

Information sharing in cybersecurity is formally embedded in Slovenia’s legal and strategic environment. Several national laws and frameworks regulate how public authorities, critical infrastructure operators, and private entities exchange threat intelligence, report incidents, and coordinate responses. These instruments align Slovenia with the EU’s cybersecurity directives while providing mechanisms for collaboration through CERTs, national coordination bodies, and sectoral regulators. The table below outlines the main policies and frameworks, with a focus on their relevance to information sharing.

Policy / Framework	Description & relevance to information sharing
Information Security Act (ZInfV-1)	Transposes the EU NIS2 Directive into Slovenian law. Defines mandatory incident reporting, cooperation among competent authorities, and structured information-sharing obligations for critical and essential service providers (Republic of Slovenia, 2025).
Cyber Security Strategy of the Republic of Slovenia	Sets the national vision for cybersecurity and highlights the need for coordination between SI-CERT, SIGOV-CERT, MoD, police, and critical infrastructure operators. Identifies information sharing as a core principle for resilience (Government of the Republic of Slovenia, 2016).
Electronic Communications Act (ZEKom-1)	Requires electronic communications operators to report incidents and cooperate with regulators and CERTs. Ensures the telecom sector is part of the national information-sharing framework (Republic of Slovenia, 2012).
SI-CERT & SIGOV-CERT Frameworks	Provide national and government CSIRT services. SI-CERT facilitates threat intelligence exchange with private/public stakeholders and EU networks; SIGOV-CERT ensures secure information flows within public administration.
National Coordination Centre for Cybersecurity (NCC-SI)	Acts as Slovenia’s hub under the EU Cybersecurity Competence Centre framework. Supports coordination at the national level and links Slovenian stakeholders to EU information-sharing platforms.
URSIV Cybersecurity Handbook (2025)	Practical guide issued by URSIV with recommendations for public and private organizations. Outlines the national

	cybersecurity system, key legislation, and best practices for risk management, incident response, and secure information exchange. Serves as a non-binding but authoritative reference for strengthening collaboration (Government Information Security Office (URSIV), 2025).
--	--

Table 6: National cybersecurity information-sharing policies and frameworks

In Slovenia, certain mechanisms for sharing information about cybersecurity incidents and threats already exist, in line with the established rules for information exchange at both the strategic and operational levels.

URSIV leads a coordination body on which meets weekly bringing together representatives from MORS, SI-CERT, SIGOV, SOVA, and others to exchange information and manage cybersecurity risks. From that level information flow to the government level and crises management system if needed.

Regular coordination among stakeholders works well at the strategic level, however it is weaker at the operational level. Information exchange among stakeholders is carried out through SI-CERT portal and the MISP platform, which provides participants with valuable threat intelligence. When combined with Security Information and Event Management (SIEM) systems, this enables more effective protection and monitoring of managed networks. There is also an analytical centre where collected information is processed and analysed. Therefore, a comprehensive, efficient, and trustworthy national system is still to be upgraded and extended to regional and private SOC.

Legislation defines reporting obligations for obliged entities, where content, timeliness and process are specified. Information sharing takes place mainly through SI-CERT portal, from the critical infrastructure sector and private companies. URSIV also plays an important role, as it is establishing a national cybersecurity hub and planning a national ISAC, providing analytical information, do reporting to the Government and communicating to the public. Defence structures are also involved, for example the Ministry of Defence with the MISP network and links to NATO environments, which is considered a good model of operational information exchange.

The effectiveness of the existing system is limited in practice when some information exchange is limited by regulations. Information exchange often takes place informally and through personal contacts, particularly in case of major incident. Trust between stakeholders remains fragile; the legal basis for information disclosure is not always clear, and participants often lack insight into how their shared data is used or analysed or missing feedback information. Some challenges are lack of interoperability between

systems, and the absence of a unified information-sharing policy that would define responsibilities, procedures, and cooperation protocols.

International cooperation in this field is well developed, and Slovenian organisations often place greater trust in foreign partners and platforms than in domestic mechanisms.

Overall, progress can be observed, especially through planned national initiatives (ISAC, MISP integrations). However, for the system to function effectively, standardised processes, a strategic approach to building trust, and a culture of secure and timely information sharing among the state, critical infrastructure operators, the private sector, and research institutions are still needed.

Key challenges:

- Undefined levels of trust among stakeholders – information is often exchanged on an ad hoc basis, without clearly defined and consistent levels of trust.
- Limited access to data for research purposes, which restricts opportunities for research institutions to analyse cybersecurity trends and support evidence-based policy development.

Opportunities and recommendations

To improve the effectiveness of the information-sharing system, it is essential to move from isolated initiatives to a structured, trustworthy, and standardised environment that supports collaboration among the state, industry, academia, and the defence sector. Based on interviews, survey results, and expert discussions, the following directions are proposed:

- Formalise the exchange of security information for both normal operations and major incident situations, ensuring that process roles are clearly defined (URSIV ↔ SI-CERT ↔ SOC). Strengthen interoperability among existing platforms, with a focus on linking URSIV, SI-CERT, MORS, and regional and private SOC's.
- Standardise procedures and protocols – implement unified trust levels (TLP) and adopt a national taxonomy aligned with international standards. Promote a culture of trust and secure information sharing through training, awareness-raising, and joint exercises.
- Strengthen national coordination and integration with European structures to ensure Slovenia remains an equal and trusted partner in information exchange and incident response.

5.2 Cybersecurity threat intelligence sharing mechanisms, platforms and tools (e.g., CERTs, ISACs)

Effective cybersecurity relies on timely and trusted threat intelligence sharing between organizations, sectors, and nations. In Slovenia, this exchange is facilitated by a combination of national CERTs, European and global networks, thematic information-sharing communities, and technical platforms that automate the flow of indicators of compromise and best practices. These mechanisms ensure that stakeholders — from government bodies to critical infrastructure operators and private industry — have access to actionable knowledge that strengthens resilience against cyber threats.

Mechanism / Platform	Description & role in information sharing
SI-CERT (Slovenian Computer Emergency Response Team)	National CERT responsible for incident response and CTI sharing with private sector and citizens. Publishes alerts, annual reports, and participates in EU/ENISA networks to exchange threat data.
SIGOV-CERT	Specialized CERT for Slovenian public administration. Coordinates incident reporting, disseminates threat intelligence, and ensures secure information flow among government institutions.
MoD Cybersecurity Centre / military CSIRT	Specialized CERT for Slovenian Ministry of Defence. Coordinates incident reporting, disseminates threat intelligence, and ensures secure information flow among government institutions.
Coordination layer	the Information & Cyber-Security Division (SIKV) inside URSIV chairs the national “CSIRT-Swift” calls and routes situational reports between SI-CERT, SIGOV-CERT, MoD and intelligence services (SOVA, Police).
European CSIRT Networks (CSIRTs Network, MeliCERTes)	Slovenia, via SI-CERT and SIGOV-CERT, participates in EU-level CERT cooperation networks. Enables cross-border CTI exchange and joint incident response exercises.
MISP (Malware Information Sharing Platform)	Open-source platform used in Slovenia (including through projects like INTERCEPT) for structured and automated sharing of indicators of compromise, TTPs, and threat data.

	Hosted by SI-CERT; free for all entities that fall under the Information Security Act
National Incident Portal	Online forms that generate STIX reports and feed MISP or the gov ticketing system.
ISACs (Information Sharing and Analysis Centres)	Emerging sectoral initiatives in finance, energy, and telecom. Provide trusted communities where operators share sector-specific CTI, vulnerabilities, and incident trends.
ENISA Platforms & Exercises (e.g., Cyber Europe)	EU-level mechanisms that integrate Slovenian teams in large-scale cyber exercises. Provide simulated environments to practice CTI sharing and cross-border coordination. Exchange of early warnings, coordinated response playbooks and indicator bundles across borders; URSIV/NCC is the Slovenian gatekeeper.
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) & Exercises	While not a platform in the narrow sense, Slovenia participates in NATO-led cyber defence exercises (e.g., Locked Shields) which focus heavily on sharing threat intelligence under operational conditions.
National Coordination Centre for Cybersecurity (NCC-Slovenia)	Serves as Slovenia's node in the EU Cybersecurity Competence Network. Facilitates connections to EU platforms, funding for CTI projects, and stakeholder coordination.
Sector SIEM "collectors"	Near-real-time enrichment of indicators for critical infrastructure (piloted in the CyberSEAS EU project). Large operators (energy, telco, finance) forward anonymised logs / IoCs to SI-CERT MISP via REST-TAXII.

Table 7: Cybersecurity threat intelligence sharing mechanisms, platforms and tools

The project participants agree that the exchange of cyber threat intelligence (CTI) in Slovenia currently relies mainly on SI-CERT and CSIRT structures, and partly on MISP, which some stakeholders see as an opportunity to improve cooperation. Individual organisations also use commercial CTI platforms or threat intelligence provided by security solution vendors, which enables basic monitoring of vulnerabilities and threats. The planned establishment of the national analytical centre ISAC is also viewed positively, as it could strengthen systematic information sharing.

However, information exchange is still often informal, fragmented, and insufficiently supported by clear processes. There is insufficient information about detected pre-

incident activities, ongoing cyber threats, and emerging trends, particularly within technical services that have limited access to broader intelligence. Unequal access to information and the absence of feedback mechanisms mean that incident reporters often do not receive updates on how their reports are handled or on the results of analyses. Moreover, there are no national platform or clear rules for cooperation, the level of trust among stakeholders is low, and information sharing is hindered by legal constraints, fear of exposure, and a lack of analytical capacity. As a result, organisations often rely on their own resources and initiatives, and cooperation at the ecosystem level remains a development opportunity.

Opportunities and recommendations

To strengthen national cybersecurity coordination and improve overall situational awareness, the following measures are proposed:

- Introduction of data collection and analysis tools within the joint situational centre.
- Improve integration between existing channels and the activities of URSIV, SI-CERT, governmental SOC down to the private SOCs, ensuring regular and coordinated communication within the framework of the national situational centre.
- Information exchange with regional and EU Cyber Hubs.
- Expand the use of MISP to all obligated entities and ensure interoperability with systems in both the public and private sectors.

5.3 International cooperation and best practices in cybersecurity information sharing

Cyber threats transcend national borders, making international cooperation in information sharing a cornerstone of effective cybersecurity. By engaging in cross-border frameworks, Slovenia not only benefits from access to timely threat intelligence and best practices but also contributes its own expertise to European and global networks. Best practices highlight the importance of trust, standardization, and joint exercises, ensuring that information exchange is both actionable and secure.

Slovenia's Role in Cross-Border Information Sharing:

- EU and ENISA Networks: Slovenia actively participates in the CSIRTs Network, MeliCERTes platform, and ENISA's Cyber Europe exercises. These initiatives allow SI-CERT and SIGOV-CERT to exchange threat intelligence with their European counterparts, harmonize response protocols, and test information-sharing under simulated attack conditions.

- NATO and Regional Cooperation: Through NATO's CCDCOE and exercises such as Locked Shields, Slovenia contributes to transatlantic cooperation in cybersecurity, where CTI sharing is central to operational readiness. Regionally, Slovenia has hosted multinational exercises (e.g., Adriatic regional cooperation events), reinforcing trust and cross-border information flows.
- EU Cybersecurity Competence Network: As part of the EU's framework, NCC-SI acts as the national coordination hub, linking domestic stakeholders with European research, innovation, and information-sharing initiatives.

Slovenian participation demonstrates alignment with international best practices:

- Trust-based communities (e.g., ISACs, CERT forums).
- Standardized formats and protocols for CTI exchange (STIX/TAXII, MISP).
- Integration of joint exercises into information-sharing practice (ENISA, NATO).
- Balancing openness with confidentiality, ensuring sensitive data is shared appropriately (TLP standards).

International cooperation in the exchange of cyber related information is recognised as an important source of knowledge, experience, and practical security solutions. Cooperation takes place through European projects, bilateral agreements, and participation in international networks, where such cooperation provides better insight into current threats and vulnerabilities, improves incident preparedness, and strengthens response capabilities. In particular, the defence sector stands out for its high level of involvement – for example, through participation in the Locked Shields exercises and project Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) under EU's PESCO arrangement, where Slovenia actively contributes to the development of joint response capabilities.

Despite these positive effects, participation in international initiatives remains inconsistent. Not all organisations are actively involved in international information sharing initiatives. Awareness of the benefits of international information exchange is uneven and, in some cases, still insufficiently developed, which limits the more active participation of some stakeholders. As a result, the sharing of experiences and good practices does not always take place systematically but often only during crisis situations. There is a clear need for greater openness, trust, and proactive involvement in international initiatives, as this directly contributes to strengthening national cyber resilience.

Summary of key challenges:

- Uneven awareness of the benefits of international information exchange – stakeholders differ in their understanding of the importance and usefulness of such cooperation.
- Limited active participation of certain stakeholders, where activities largely depend on individual initiatives.
- Unsystematic exchange of experiences and good practices, which often occurs only during crisis events or within project-based frameworks.
- Lack of a national-level coordination mechanism that would connect key actors and ensure continuous communication and information exchange.
- Low level of trust and absence of clear procedures for information protection, which limits openness and willingness to share data.
- Excessive fragmentation, as several isolated “sandbox” initiatives exist without interconnection, reducing national coherence and alignment.

Opportunities and recommendations For Slovenia to participate more effectively in international information exchange, it is essential that international cooperation evolves from isolated initiatives into a continuous, institutionally supported practice involving all key sectors – governmental, defence, industrial, and academic. Based on the findings the following directions are proposed:

- Expand the role of the existing National Coordination Centre (NCC) to serve as a national coordination mechanism and connecting platform among government bodies, critical infrastructure operators, industry, and the research community, ensuring active participation in international information exchange and cooperation with global partners.
- Strengthen communication and coordination among national institutions (URSIV, SI-CERT, MORS, SOVA) and with key international partners.
- Ensure Slovenia’s regular participation in international exercises (e.g. Locked Shields, NATO and EU cyber exercises) and expand involvement in European initiatives focused on the exchange of operational experiences.
- Develop a programme of workshops and training to facilitate the transfer of good practices from the international environment into the national system.
- Promote a culture of cooperation and trust among stakeholders – moving away from a “state versus private sector” mindset towards shared responsibility and common goals.
- Enhance the role of CCIS in involving the business sector in international initiatives and linking it with European networks.

Through coordinated action, greater openness, and a systematic approach to knowledge and experience sharing, Slovenia could become a more visible and reliable partner in the European and global cybersecurity landscape.

5.4 Challenges in cross-sectoral information sharing

The new ZInfV-1 (Republic of Slovenia, 2025) introduces a significantly expanded framework for cybersecurity governance in Slovenia, with a particular emphasis on structured information sharing and incident reporting across sectors. The regulation establishes new obligations for public institutions, critical infrastructure operators, and private entities, aiming to enhance coordination and resilience within the national cybersecurity ecosystem.

A key change of ZInfV-1 (Republic of Slovenia, 2025) is the formal regulation of information exchange within interconnected supply chains, reflecting the growing importance of cross-sectoral dependencies in managing cyber risks. While the legal foundations are now in place, the practical implementation of these mechanisms—through dedicated platforms, automated threat intelligence exchange, and cross-sectoral cooperation—remains in progress.

Many organisations, particularly smaller entities such as SMEs and local public bodies, will require time, resources, and guidance to adapt to the new requirements.

Information sharing between different sectors in the field of cybersecurity is recognised as essential for effective response to threats, but in practice it faces several challenges. Although some mechanisms exist, such as occasional forums or technical bulletins, a systemic approach has not yet been established. As a result, cooperation is often limited to urgent cases or based on personal connections.

What works well: In some areas, progress in cooperation can be observed. URSIV acts as a formal coordinator, and certain coordination forums and information bulletins are in place. At the technical level, data on vulnerabilities and indicators of compromise (IoCs) are exchanged, and the sharing of practical experience during incidents is considered useful. Cooperation based on trust, such as joint responses to major cyber incidents, is also viewed positively.

Key challenges:

Despite existing initiatives, cross-sector information exchange is often hindered due to:

- Limited trust – while cooperation during incident response has improved, many companies and organisations are reluctant to share information for fear of reputational damage or exposing vulnerabilities. A culture of systematic experience sharing is still insufficiently developed
- Absence of unified platforms and standards – there is no national mechanism or platform for secure and structured information sharing available to all organisations.
- Fragmented ecosystem – information exchange is uncoordinated, often informal, and dependent on personal networks or crisis situations.
- Competing interests and “silo mentality” – individual sectors or organisations keep information to themselves due to business interests or competition.
- Lack of incentives and weak connectivity among actors from industry, the public sector, and academia.
- Insufficient exchange of good practices.
- Different levels of maturity and awareness – less mature organisations often lack the capacity to participate or do not recognise the added value of sharing information.

Opportunities and recommendations:

- Promote cross-sector information sharing on security incidents – encourage the exchange of case examples and response measures among sectors to strengthen collective learning and build a repository of lessons learned.
- Facilitate peer-to-peer experience exchange – enable practitioners who handle incidents operationally to share their experiences, methods, and lessons directly with others.
- Formalise cooperation at the operational level – establish structured frameworks or protocols to connect operational teams across sectors and ensure continuous coordination beyond ad-hoc or project-based interactions.

5.5 Other informal information and knowledge sharing instruments

Formal cybersecurity frameworks in Slovenia provide the backbone for information exchange, but in practice, much of the knowledge sharing also happens through informal instruments. These rely on professional trust, networking, and community-driven initiatives, which often enable faster, more candid, and more practical exchanges than official reporting channels. Such instruments play a complementary role, bridging gaps

between institutions and fostering a culture of collaboration in the cybersecurity ecosystem.

Instrument	Examples in Slovenia	Role in information sharing
Professional associations and chambers	SeKV – ICT Association (ZIT), Slovensko društvo informatika, ISACA Slovenia	Provide forums, working groups, and mailing lists where practitioners exchange experiences, alerts, and best practices. Create spaces for networking, case study presentations, and informal knowledge transfer across sectors.
Conferences and workshops	Infosek, Cyber Conferences, Dnevi slovenske informatike	Create spaces for networking, case study presentations, and informal knowledge transfer across sectors.
Communities of practice & expert networks	Sector-based expert groups in banking, telecoms, energy	Operate as trusted circles of professionals who share sensitive alerts quickly through personal and sectoral networks.
Academic and student initiatives	Hackathons (CyberNight, DigiHack), CTF competitions, student research groups	Encourage informal peer-to-peer learning and exchange of cybersecurity knowledge among the next generation of experts.
Social media and online forums	LinkedIn groups, local forums, closed channels (e.g., Signal, Slack groups)	Facilitate rapid, ad-hoc sharing of information, early warnings, and professional discussions outside formal structures.

Table 8: Other informal information and knowledge sharing instruments

In Slovenia, informal information exchange plays an important role in responding to cybersecurity incidents. The relatively small size of the community and the close professional connections among experts enable rapid communication through trusted personal networks – the so-called “phonebook system.” These channels often fill the gaps that formal mechanisms have not yet addressed, especially in the cases of critical incident/situations, where quick action is essential.

The most commonly used informal instruments are professional associations, personal networks, and industry conferences, which facilitate the sharing of experience and

operational information. While this approach enhances responsiveness, it is also considered risky in the long term, as it is not supported by uniform procedures or clearly defined responsibilities.

Key challenges:

Informal channels rely heavily on trust and personal connections, which bring both advantages and weaknesses:

- Lack of formal structure and rules often means that discussions do not lead to concrete actions or follow-up, as roles and procedures are not formally defined.
- Unequal access to information and excessive reliance on personal contacts reduce transparency and hinder broader stakeholder participation and knowledge transfer.

Opportunities and recommendations

To improve the overall effectiveness of information exchange, informal cooperation should be strengthened and enhanced through more structured solutions, rather than replaced.

- Develop sector-specific forums and digital platforms that maintain the trust and speed of informal networks while ensuring traceability and inclusiveness.
- Foster a culture of collaboration and shared responsibility, where informal exchanges complement formal processes and contribute to a stable, reliable national system for information sharing.

6 Analysis of dual-use technologies

This section explores the intersection between cybersecurity technologies that have applications in both civilian and defence contexts. It discusses the implications of dual-use technologies for national security, innovation, and regulatory compliance.

6.1 Definition and importance of dual-use cybersecurity technologies

Dual use originally refers to the export of goods and technologies that can be used for both civilian and military purposes. This area is regulated by EU rules, such as Regulation

(EU) 2021/821 (European Union, 2021a), which establishes the Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items.

The dual use of technologies—that is, the **application of innovations** for both civilian and defence or security purposes—also represents an opportunity for the Slovenian innovation ecosystem. It can serve as a driver of innovation, internationalisation, and greater resilience of the national economy and society as a whole.

Dual-use technologies in cybersecurity represent a strategic opportunity to strengthen national resilience, accelerate innovation, and foster cooperation between the civilian and defence sectors. They enable more efficient use of resources, support economic and technological development, and enhance strategic autonomy through domestic expertise.

The civilian sector — as the main driver of technological progress — plays a crucial role in developing solutions applicable to both civil defence and military operations. Dual-use innovation also facilitates participation in European projects and access to international funding.

Key challenges

Despite its potential, the development of dual-use cybersecurity technologies in Slovenia faces several interconnected challenges. Cooperation is further hindered by low mutual trust and limited knowledge exchange between sectors, largely due to differing standards and the closed nature of military systems.

Opportunities and recommendations

To realise the potential of dual-use technologies, Slovenia should strengthen cooperation between the civilian, industrial, and defence domains through targeted policy, coordination, and capacity-building measures. Key opportunities and actions include:

- Adopting a unified national framework that connects economic, research, and defence goals, defining coordination mechanisms, funding priorities, and technology transfer pathways.
- Promoting joint R&D initiatives between civilian and defence actors, focusing on areas such as critical infrastructure protection, secure communications, and advanced threat analysis.
- Enhancing institutional cooperation between MORS, URSIV, and CCIS to identify strategic projects and secure European or international funding.

- Building mutual trust and understanding through joint exercises, workshops, and transparent knowledge exchange to strengthen national resilience and technological competitiveness.

6.2 National policies and frameworks governing dual-use cybersecurity solutions

Cybersecurity technologies fall into the category of *dual-use* goods – tools and software that can serve both civilian and military purposes (e.g., strong cryptography, network monitoring systems, intrusion tools...). Based on EU Regulation 2021/821 (European Union, 2021a) setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, Slovenia has updated its legislation. This law determines national competences, procedures, penalties and supervisory authorities. – supplements and implements the European regulation.

Policy / Framework	Description & relevance to dual-use cybersecurity
Dual-Use Goods Export Control Act (ZNIBDR)	Regulates the export of goods, software, and technology with both civilian and military applications. Cybersecurity tools such as advanced encryption or intrusion software may require an export license before being transferred outside the EU (Republic of Slovenia, 2004).
Defence-Related Goods Export Control Act (ZNIBOMN)	Focuses specifically on military equipment and defence-related technologies. Applies to cybersecurity solutions with clear defence applications, ensuring exports are strictly controlled and licensed by the Ministry of Defence (Republic of Slovenia, 2011).
Information Security Act (ZInfV-1, 2025)	Implements the EU NIS2 Directive in Slovenia. While not an export control law, it defines obligations for critical entities and regulates the secure handling of sensitive technologies, ensuring responsible use within national borders (Republic of Slovenia, 2025).
National Security Strategy (ReSNV-2, 2019)	Identifies hybrid and cyber threats as key risks to Slovenia’s security. Establishes principles of resilience and controlled information exchange, which indirectly

	guide how dual-use cybersecurity solutions are governed (Government of the Republic of Slovenia, 2019)
International and EU Commitments	Slovenia implements EU Regulation 2021/821 (European Union, 2021a) on dual-use items and adheres to international export control regimes (e.g., Wassenaar Arrangement) (Wassenaar Arrangement Secretariat, 2025)). These commitments align national practice with global standards on controlling sensitive cybersecurity tools.
Regulation on the procedure for issuing licenses and certificates and on the role of the Commission for the Dual-Use Goods Export Control	Defines the documentation and procedures for issuing licenses, certificates, and transit prohibitions, and sets the tasks and operation of the Commission for the Dual-Use Goods Export Control Act. It also covers reporting, record-keeping, restrictions on EU general export licenses, and measures to ensure compliance with EU Regulation 428/2009 (European Union, 2009).

Table 9: National policies and frameworks governing dual-use cybersecurity solutions

The national framework for dual-use in cybersecurity is based on the European dual-use regulation, which governs control and customs procedures for the transfer of sensitive technologies. However, in practice, there is no unified and clearly communicated national policy that would cover all relevant aspects. The civilian sector is often the source of dual-use technologies, which means significant development opportunities exist — for example, existing solutions such as cryptographic systems or hardware security modules (HSM) can be used for both civilian and defence purposes, enabling participation in European programmes and commercialisation.

At the same time, important gaps are visible: while export control rules are clearly defined, there is a lack of specific guidelines and awareness regarding dual-use innovations, particularly in terms of technology transfer from research to industry and the absence of national incentives to accelerate the development of dual-use products of national interest.

To fully leverage the potential of dual-use technologies without increasing security risks, clearer national guidance, simplified procedures, and stronger coordination between the state, research institutions, and industry are needed — supported by a coherent strategic framework that fosters healthy competition, rapid progress, and reasonable export control

measures, positioning dual-use innovation as a driver of competitiveness, resilience, and international cooperation.

6.3 Challenges in regulating and managing dual-use technologies

The regulation of dual-use cybersecurity technologies in Slovenia is aligned with European legislation and primarily focuses on export control and the supervision of sensitive technologies. These mechanisms ensure compliance with EU requirements but only partially address the promotion of innovation and technology transfer. The current framework does not sufficiently stimulate the development of commercial products that meet military standards or upgrade the products and support the broader innovation ecosystem.

The defence sector remains a closed environment by nature, limited by strict security requirements, while most development activity takes place in the civilian domain. Nevertheless, efforts have been made to increase accessibility through open events, joint projects, and initiatives that encourage collaboration between defence institutions and industry. The implementation of certification processes has also helped clarify operational requirements and technical standards.

Key challenges

Managing and developing dual-use technologies in cybersecurity remains complex due to several interrelated factors. While export controls and compliance mechanisms are well-established, national policy lacks a strategic framework that would guide cooperation and innovation across sectors.

Awareness of the role of cybersecurity in national defence and within alliances, where cyberspace has become one of the domains of hybrid warfare, may not yet have matured to the level at which stakeholder cooperation would enable a clear strategy and foster faster joint development of innovations and tools essential for the protection of the digital society.

Regulatory and legal barriers continue to limit the transfer of knowledge and technology from research to industry, and there is a low level of awareness among stakeholders regarding existing rules and procedures. Some activities are limited due to the public procurement regulations.

In addition, the lack of international cooperation and alignment with European partners constrains knowledge exchange and reduces access to cross-border innovation opportunities. Well established program at EDA CapTech Cyber is developing slowly due the lengthy coordination procedures from the initiative to the start of the project (European Defence Agency (EDA), 2025).

Moreover, the balance between export restrictions and the promotion of dual-use innovation is not yet clearly enough defined, resulting in uncertainty for companies interested in developing defence-compatible solutions.

The lack of maturity in recognising cybersecurity's role in national defence and what products for national procurement make sense to develop nationally and what remains to be done with the import of technologies that will not affect the resilience of national infrastructure. These challenges risk perpetuating dependence on foreign technologies and reducing the resilience of domestic infrastructure.

Opportunities and recommendations

To improve the management of dual-use technologies and foster innovation, Slovenia should focus on a more integrated and enabling regulatory environment. Key opportunities and actions include:

- To formulate a strategy for the development of dual-use products based on future defence requirements and the development of national research and development capabilities.
- The industry has to form its interest and strategy for cooperation in the development of dual-use products at the association level.
- To enforce the development and use of testing capabilities to ensure cybersecurity throughout the product lifecycle of dual-use products.
- Include clearer certification processes for defence applications in knowledge and technology transfer procedures.
- Expanding the regulatory framework to include incentives and mechanisms for adapting and developing dual-use technologies within the national innovation ecosystem.
- To establish proper regulation for respect of international humanitarian law and provide clear definitions or rules for cyber weapons and dual-use technologies in armed conflict. The lack of legal clarity creates a grey zone where actions cannot be easily judged as lawful or unlawful, weakening norms and accountability mechanisms.
- Ensuring responsible development and deployment requires inclusive dialogue, raising national awareness and stronger societal oversight mechanisms and

appropriate regulation of the use of cybersecurity technologies in a defence organization.

- Strengthening participation in European programmes (e.g. EDF, CapTech Cyber, NATO initiatives) with coordinated support from national institutions to align funding and innovation efforts with EU priorities

A coordinated and innovation-oriented approach would allow Slovenia to better leverage its civilian expertise, promote domestic technological development, and strengthen its position within the European dual-use and cybersecurity landscape.

6.4 Examples of cybersecurity technologies with dual-use applications

In Slovenia, dual-use cybersecurity technologies are most often found in the areas of cryptography, threat detection, and data analysis algorithms, where their applications are relevant for both civilian and defence environments. A prime example is the development of an encryption device (Xiphra Core Encryptor 10G) that has been included on the list of "NATO-approved" cryptographic devices that are security-appropriate for protecting NATO classified information. Commercial solutions are frequently adapted for critical infrastructure protection or for defence and military use, demonstrating the potential for synergy between sectors (North Atlantic Treaty Organization (NATO), 2025).

The cyber range infrastructure is another clear example of dual-use capability, serving as a shared platform for training, testing, and simulation in both industrial and defence contexts. Although the number of recognised domestic cases remains limited, awareness of this potential is growing, and dual-use technologies are increasingly seen as an opportunity to enhance national resilience and innovation capacity.

The development and use of these technologies are hindered by the lack of structured cooperation mechanisms between the civilian and defence sectors. Companies remain cautious about engaging in defence-related projects due to regulatory uncertainty, limited understanding of military requirements, and complex legal conditions for technology transfer. Despite these limitations, dual-use technologies are recognised as an important opportunity for strengthening national resilience and innovation potential.

Opportunities and recommendations

To strengthen the ecosystem for dual-use cybersecurity technologies, Slovenia should improve coordination and encourage applied research that bridges civilian and defence applications. Key actions include:

- Establishing a national framework for technology transfer and collaboration, ensuring that R&D outcomes can be efficiently adapted for both civil and defence needs.
- Encouraging cooperation between academia, industry, and defence stakeholders to identify practical dual-use use cases.
- Raising awareness among companies and innovators about dual-use opportunities, clarifying legal and ethical aspects, and showcasing successful domestic examples.

With a more coordinated approach, dual-use technologies could become a key driver of Slovenia's cybersecurity innovation, helping to bridge the gap between research, industry, and defence.

7 Policy recommendations

The Information Security Act (Republic of Slovenia, 2025) addresses the minimum requirements that entities must meet to ensure cybersecurity. Considering the chronic shortage of qualified personnel, participants in the study were largely united in recognising the urgent need to update the National Cybersecurity Strategy (Government of the Republic of Slovenia, 2016) and to agree on implementation programme optimizing the resources usage. Such an updated strategy should encourage society to continue developing resilience and preparedness for response, including in times of crisis or emergency.

Clear and measurable objectives, supported by an implementation programme, are only a starting point — what is essential is active participation within the cybersecurity ecosystem. This means engaging in a network of public, private, and research stakeholders who exchange knowledge, data, and technologies to collectively strengthen cyber resilience, foster innovation, and protect the digital society. Cybersecurity must be established as a systemic domain, where no single organisation can manage all threats on its own.

Improved cooperation would enable:

- faster responses to cyber incidents and more effective recovery in the event of breaches,
- better sharing of resources and expertise, given that resources are limited and often underutilised,

- increased resilience of digital infrastructure through the faster implementation of preventive measures,
- more rapid development of national capabilities to handle complex incidents and crises,
- joint innovation and access to funding programmes,
- faster and more effective achievement of compliance with legislation e.g. NIS2 (European Union, 2022a), CRA (European Union, 2023), DORA (European Union, 2022b).

7.1 Strengthening national cybersecurity governance

Given the outdated nature of the national cybersecurity strategy, several recommendations are proposed:

1. In addition to the existing weekly coordination among state authorities, it is important to establish coordination at the strategic level, which will enable the inclusion of industry — both research and development (R&D) organisations and providers of cybersecurity products and services.
2. Raise the level of operational capabilities by strengthening cooperation between the state, industry, and academia — establishing clear leadership, structured processes, and the exchange of security information and experiences at the operational level.
3. Increase investment and political support — ensure stable funding for infrastructure, research, innovation, and dual-use technologies, as well as incentives for the implementation of cybersecurity measures in the defence industry.
4. Workforce development must attain strategic importance to enable both short-term and long-term solutions to the problem of skills shortages. It is necessary to define appropriate profiles, career paths, and their implementation in human resource management. To attract and retain professionals, adequate conditions should be ensured that correspond to the needs of different professional profiles, while also addressing intergenerational characteristics.
5. Promote the active participation of Slovenian experts in international networks and exercises and strengthen cooperation between research and industrial partners in international R&D consortia.
6. The strategy should define clear and measurable objectives, deadlines for their achievement, and responsibilities. It should be adopted together with an action plan that includes measures, tasks, and projects with allocated resources and defined accountability for implementation within specified timeframes.

7. Develop a cybersecurity culture through continuous awareness campaigns, encouraging appropriate daily practices from the individual to management level.

7.2 Enhancing technology transfer mechanisms

Technology transfer and information sharing are essential in cybersecurity to ensure that knowledge, tools, and best practices are effectively shared among stakeholders such as governments, private companies, and research institutions.

Among the existing mechanisms of technology transfer, the use of foreign software through licensing agreements remains predominant. Public-private partnerships (PPPs) in the field of cybersecurity have not yet become established. Exceptions exist around spin-offs and start-ups, while the primary mechanism for cooperation continues to be participation in R&D projects.

In technology transfer, greater emphasis should be placed on the business dimension within R&D organisations and on building stronger links with companies, for example through patents or the commercialisation of knowledge. Alternatively, companies should take the initiative and highlight development requirements. Both parties shall address the underlying causes of limited collaboration—such as the closed nature of universities and the reluctance of businesses to engage.

Participants have proposed the preparation of a strategic document, accompanied by an implementation programme or action plan, to introduce open topics as follows:

- A strategic body to promote cooperation between companies, R&D organisations, and the government, and to develop a research and development programme in cybersecurity, including aspects of dual-use technologies.
- Simplify administrative procedures and reduce bureaucratic barriers that discourage participation in national R&D projects.
- Renewing incentives to encourage more active involvement of both R&D organisations and companies in R&D projects.
- Recognise and reward successful technology transfer and commercialisation outcomes as integral components of research evaluation frameworks.
- Establishing mechanisms to ensure transparency in the allocation of resources and the outcomes of projects.
- Strengthening the resources of intermediary institutional organisations, such as SRIPs or clusters/competence centres, whose key role is to support R&D projects from the idea stage through to implementation in operational practice.

- Promote a multidisciplinary approach to education and training to enhance collaboration, foster innovation, and align skills with the evolving needs of industry and society. Strengthen programmes that integrate dual-use and cybersecurity components to develop a highly skilled and adaptable workforce.
- Develop a comprehensive national strategy for cybersecurity and dual-use research and innovation that links academia, industry, and defence. The strategy should define clear objectives, priority technologies, and stable funding mechanisms, supported by transparent legal and procedural frameworks that enable civilian participation in national and defence-related projects, simplify administrative processes, and ensure long-term impact.

Technology transfer and information sharing are critical in cybersecurity to ensure that knowledge, tools, and practices are effectively disseminated among stakeholders such as governments, private companies and research institutions.

7.3 Improving information sharing practices

Slovenia has established the basic building blocks for cybersecurity information sharing. The foundation is based on the Information Security Act (ZInfV-1) (Republic of Slovenia, 2025), which requires entities to report incidents. At the governmental level, regular information exchange is taking place, while for the general public, SI-CERT provides a portal offering information on threats and vulnerabilities, as well as access to the national MISP platform.

To enhance information sharing, the following recommendations are proposed:

- Formalise and enhance information exchange procedures for both routine operations and critical security incidents, ensuring feedback mechanisms for incident reporters and systematic sharing of lessons learned – including insights from operational experiences, R&D outcomes, and best practices.
- Improve procedural roles and information exchange between the strategic level and security operations centres (including private SOC's).
- Establish regular communication mechanisms among public authorities, critical infrastructure operators, companies of national security relevance, cybersecurity service providers, and research organisations, while strengthening both formal and informal operational-level collaboration networks.
- Expand the use of the MISP platform.
- Increase the visibility of the national ISAC as a source of analytical and intelligence information.

- Enhance active involvement in international networks and ensure effective dissemination of information, best practices, and experiences to national stakeholders.

7.4 Managing dual-use cybersecurity technologies

The civil sector is the main source of dual-use technologies, with significant innovation potential for developing defence capabilities, protection, and crisis response. It enables the growth of domestic expertise, strengthens strategic autonomy, and increases the resilience of critical infrastructure. To accelerate the development of this increasingly important field, which contributes both to enhancing defence capabilities and achieving broader societal development goals, the following improvements are proposed:

- Develop a national strategy and implementation programme that reflects national needs and development opportunities while stimulating innovation activities.
- Establish cooperation mechanisms at both strategic and operational levels with the defence sector and the military, aimed at building trust, exchanging relevant technological information, understanding operational challenges and standards, and facilitating knowledge transfer for the development of successful dual-use products.
- Define a clear national direction and practical guidelines to enable more effective cooperation between the defence sector, the research community, and industry.
- Raise awareness within industry about the long-term nature of dual-use product development, as only a gradual process from idea to final operational product can meet the demanding standards of the defence sector.
- Continue building on best practices and experiences from participation in national and European research and development projects (e.g. EDA CapTech Cyber, EDF, NATO DIANA) and joint cybersecurity exercises (e.g. Locked Shields, Cyber Night).
- Establish a formal cooperation agreement between the defence sector and industry (including companies and R&D institutions), coordinated under the auspices of the ICT Association at the CCIS, to provide a structured framework for engagement.
- Develop regular and institutionalised mechanisms for collaboration, such as joint working groups, strategic forums, or coordinated project calls, to ensure sustained and effective interaction between stakeholders.

8 Conclusions

The Slovenian case study confirms that the country has made significant progress across all key areas of cybersecurity — from the establishment of a normative framework to tangible results in preventive and corrective operations. The study itself has played an active role in fostering dialogue between the defence sector and industry, encouraging more structured discussions on mutual cooperation and technology development.

The implementation of the study's activities has contributed to intensified communication between defence institutions and industry, resulting in concrete outcomes such as industry participation in the education and training programme *"Leadership, Research and Innovation in Defence Organisations – Strategic Approaches and Practical Cases"*, collaboration during the *4th Military Science Days*, and the participation at the *Cybersecurity Panel* at the *SIDEC 2025* conference.

The analysis also highlights that further progress can only be achieved through enhanced active cooperation among stakeholders at all levels. Shared objectives should be clearly articulated in the updated National Cybersecurity Strategy, serving as a foundation for coordinated national action. By optimising activities, Slovenia can ensure more efficient use and development of its human resources — one of the key obstacles identified during the study.

The achieved cooperation between defence and civil sectors in joint R&D projects and joint exercises has proven to be an excellent basis for building trust and strengthening future collaboration. These partnerships shorten the time from idea to operational implementation, increasing the country's overall cyber readiness. The study has also identified several untapped opportunities that can be further integrated into cooperation programmes.

In conclusion, Slovenia is well positioned to build on these achievements. The next step lies in transforming strategic declarations into clear, actionable programmes supported by persistent operational efforts. A coherent, trust-based and goal-oriented approach will enable Slovenia to enhance its cybersecurity ecosystem and contribute more effectively to the European cybersecurity community.

9 Annexes

This section includes any additional supporting documents, data, or reference materials that provide further context for the case study. It may include a glossary of terms, a list of acronyms, interview transcripts, survey results, or references to relevant legislation and policy documents.

9.1 References and bibliography

- European Commission. (2025). European Commission – Cybersecurity Atlas. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-atlas>
- European Defence Agency (EDA). (2025). EDA Capability Technology Groups – CapTech Cyber. <https://eda.europa.eu/what-we-do/technology-and-capabilities/capability-technology-groups>
- European Union. (2009). Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009R0428>
- European Union. (2021a). EU Dual-Use Regulation (EU) 2021/821. <https://www.eur-lex.europa.eu/eli/reg/2021/821>
- European Union. (2021b). European Defence Fund – Legal Framework / Regulation establishing the EDF. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0697>
- European Union. (2022a). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). <https://eur-lex.europa.eu/eli/dir/2022/2555>
- European Union. (2022b). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). <https://www.eur-lex.europa.eu/eli/reg/2022/2554>
- European Union. (2023). Regulation (EU) 2023/1230 on Machinery (Cyber Resilience Act – CRA). <https://www.eur-lex.europa.eu/eli/reg/2023/1230>
- European Union Agency for Cybersecurity (ENISA). (2024). ENISA. Cyber Europe 2024 – After Action Report. <https://www.enisa.europa.eu/publications/cyber-europe-2024-after-action-report>
- Government Information Security Office (URSIV). (2025). URSIV Cybersecurity Handbook (2025).
- Government of the Republic of Slovenia. (2016). Cybersecurity Strategy of the Republic of Slovenia (2016).

- <https://www.gov.si/assets/ministrstva/MPJU/DID/Kibernetska-varnost/Cyber-Security-Strategy-of-the-Republic-of-Slovenia-2016.pdf>
- Government of the Republic of Slovenia. (2019). National Security Strategy of the Republic of Slovenia (ReSNV-2).
<https://www.gov.si/assets/ministrstva/MO/Dokumenti/ReSNV2.pdf>
 - Government of the Republic of Slovenia. (2023a). Digital Slovenia 2030 Strategy.
https://www.gov.si/assets/ministrstva/MDP/Dokumenti/DSI2030-potrjena-na-Vladi-RS_marec-2023.pdf
 - Government of the Republic of Slovenia. (2023b). Resolution on the Slovenian Scientific Research and Innovation Strategy 2030 (ZRISS 2030).
https://www.gov.si/assets/organi-v-sestavi/URSIL/Dokumenti/NACIONALNA-STRATEGIJA_IL_EN_ebook.pdf
 - Government of the Republic of Slovenia. (2024). National Intellectual Property Strategy 2030. <https://www.gov.si/novice/2024-03-21-strategija-intelektualne-lastnine-do-let-2030/>
 - Ministry of Defence of the Republic of Slovenia. (2020). The Resolution on the General Long-Term Development and Equipping Program of the Slovenian Armed Forces until 2040 (ReDPROSV40).
<https://www.gov.si/assets/ministrstva/MO/Dokumenti/Informacija-o-impementaciji-ReDPROSV40-1.pdf>
 - Ministry of Defence of the Republic of Slovenia. (2023). Medium-term Defence Programme of the Republic of Slovenia 2023–2028 (SOPR 2023–2028).
https://www.slovenskavojska.si/fileadmin/user_upload/Slike/O_vojski/Podatki_in_dejstva/Dokumenti/SOPR_2023-2028_sprejet.pdf
 - Ministry of Higher Education, S. and I. (Slovenia). (2022). Programme of Collaborative R&D Projects and Other Projects Subject to State Aid 2022–2030.
<https://www.gov.si/assets/ministrstva/MVZI/Znanost/Strategije-predpisi-in-drugi-dokumenti/Program-sodelovalnih-raziskovalno-razvojnih-projektov-in-drugih-projektov-ki-so-predmet-drzavnih-pomoci-MVZI-2022-2030.pdf>
 - North Atlantic Treaty Organization (NATO). (2025). NATO Information Assurance Product Catalogue (NIAPC). <https://infosec.nato.int/NIAPC>
 - Republic of Slovenia. (1993). Higher Education Act (ZViS).
<https://pisrs.si/pregledPredpisa?id=ZAKO172>
 - Republic of Slovenia. (1995). Copyright and Related Rights Act (ZASP).
<https://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO403>
 - Republic of Slovenia. (2001). Industrial Property Act (ZIL-1).
<https://pisrs.si/pregledPredpisa?id=ZAKO1668>
 - Republic of Slovenia. (2004). Dual-Use Goods Export Control Act (ZNIBDR).
<https://pisrs.si/pregledPredpisa?id=ZAKO3937>

- Republic of Slovenia. (2006). Companies Act (ZGD-1).
<https://pisrs.si/pregledPredpisa?id=ZAKO4291>
- Republic of Slovenia. (2011). Defence-Related Goods Export Control Act (ZNIBOMN). <https://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6288>
- Republic of Slovenia. (2012). Electronic Communications Act (ZEKom-1).
<https://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5760>
- Republic of Slovenia. (2015). Public Procurement Act (ZJN-3).
<https://pisrs.si/pregledPredpisa?id=ZAKO7086>
- Republic of Slovenia. (2018). Information Security Act (ZInfV).
<https://pisrs.si/pregledPredpisa?id=ZAKO7707>
- Republic of Slovenia. (2021). Law on Scientific Research and Innovation Activities (ZZrID). <https://pisrs.si/pregledPredpisa?id=ZAKO7733>
- Republic of Slovenia. (2025). Information Security Act (ZInfV-1).
<https://pisrs.si/pregledPredpisa?id=ZAKO8934>
- Wassenaar Arrangement Secretariat. (2025). Wassenaar Arrangement.
<https://www.wassenaar.org/>

9.2 List of relevant organisations, initiatives, and projects mentioned in the document

Acronym	Name	Website
AI4SI	Artificial Intelligence for Slovenia Initiative	https://ai4si.gzs.si/en
AKOS	Agency for Communication Networks and Services of the Republic of Slovenia	https://www.akos-rs.si/
ARIS	Slovenian Research and Innovation Agency	https://www.aris-rs.si/
ARNES	Academic and Research Network of Slovenia	https://www.arnes.si/en/
CapTech Cyber	EDA Capability Technology Group – Cyber	https://eda.europa.eu/what-we-do/technology-and-capabilities/capability-technology-groups/captech-cyber
CCIS	Chamber of Commerce and Industry of Slovenia	https://eng.gzs.si/
CRRT (EU PESCO)	EU Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (EU project)	https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/
Cyber Europe	ENISA Cyber Europe Exercises	https://www.enisa.europa.eu/topics/training-exercises/cyber-europe-programme
CyberHubs	European Network of Cybersecurity Skills Hubs (EU project)	https://cyberhubs.eu/
CyberSEAS	Cyber Securing Energy Data Services (EU project)	https://www.cyberseas.eu/
Cybersecurity Atlas	European Commission Cybersecurity Atlas	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-atlas
DIGI-SI (EDIH)	European Digital Innovation Hub Slovenia	https://www.digi-si.eu/
ECCC	European Cybersecurity Competence Centre	https://cybersecurity-centre.europa.eu/

ECSSO	European Cyber Security Organisation	https://ecs-org.eu/
EDA	European Defence Agency	https://eda.europa.eu/
EDF	European Defence Fund	https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en
ENISA	European Union Agency for Cybersecurity	https://www.enisa.europa.eu/
ICS	Institute for Corporate Security Studies	https://www.ics-institut.si/en
IJS (JSI)	Jožef Stefan Institute	https://www.ijs.si/ijsw
INTERCEPT	Incident Response Through Threat Intelligence & Cross-border Cooperation (EU project)	https://www.cert.si/en/intercept-incident/
Locked Shields	NATO CCDCOE Locked Shields Cyber Exercise	https://ccdcoe.org/exercises/locked-shields/
MDP	Ministry of Digital Transformation	https://www.gov.si/en/state-authorities/ministries/ministry-of-digital-transformation/
MeliCERTes	MeliCERTes & MeliCERTes 2 EU Platforms (EU project)	https://digital-strategy.ec.europa.eu/en/policies/melicertes
MGTS	Ministry of the Economy, Tourism and Sport	https://www.gov.si/en/state-authorities/ministries/ministry-of-the-economy-tourism-and-sport/
MKRR	Ministry of Cohesion and Regional Development	https://www.gov.si/en/state-authorities/ministries/ministry-of-cohesion-and-regional-development/
MORS	Ministry of Defence of the Republic of Slovenia	https://www.gov.si/en/state-authorities/ministries/ministry-of-defence/
MVZI	Ministry of Higher Education, Science and Innovation	https://www.gov.si/en/state-authorities/ministries/ministry-of-higher-education-science-and-innovation/

NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	https://ccdcoe.org/
NCC-SI	National Coordination Centre for Cybersecurity Slovenia	https://cybersecurity-centre.europa.eu/ncc-slovenia_en
SI-CERT	Slovenian Computer Emergency Response Team	https://www.cert.si/
SIGOV-CERT	Governmental CERT (SIGOV-CERT Division, URSIV)	https://www.gov.si/en/state-authorities/government-offices/government-information-security-office/about-the-office/sigov-cert-division/
SOVA	Slovenian Intelligence and Security Agency	https://www.gov.si/en/state-authorities/bodies-within-ministries/slovenian-intelligence-and-security-agency/
SPIRIT	Public Agency for Entrepreneurship, Internationalization, Foreign Investments and Technology	https://www.spiritslovenia.si/en
SPS	Slovene Enterprise Fund	https://podjetniskisklad.si/en
SRIP GoDigital	Strategic Research and Innovation Partnership – ICT	https://sripgodigital.gzs.si/
UL	University of Ljubljana	https://www.uni-lj.si/
UL FDV	Faculty of Social Sciences, University of Ljubljana	https://www.fdv.uni-lj.si/en
UL FRI	Faculty of Computer and Information Science, University of Ljubljana	https://www.fri.uni-lj.si/en
UM	University of Maribor	https://www.um.si/en
UM FERI	Faculty of Electrical Engineering and Computer Science, University of Maribor	https://feri.um.si/en/
URSIV	Government Information Security Office of the Republic of Slovenia	https://www.gov.si/en/state-authorities/government-offices/government-information-security-office/
ZAG	Slovenian National Building and Civil Engineering Institute	https://www.zag.si/en

9.3 Background literature

Various sources were consulted during the preparation of this document; however, they are not cited in the text.

- Čehič Limoni, B. (2025). Povezovanje civilnega in vojaškega sektorja z namenom zagotavljanja kibernetске varnosti na območju Republike Slovenije: magistrsko delo. University of Ljubljana. <https://dk.um.si/IzpisGradiva.php?lang=slv&id=92346>
- Grm, M. (2023). Nadzor blaga z dvojno rabo – pravna regulacija v Republiki Sloveniji. Revija Pamfil. <https://revijapamfil.si/>
- Jelušič, J. (2020). Security Perception and Security Policy in Slovenia. NATO/EU Security Studies. (PDF source: "The NATO and EU Relations of Central-Eastern Europe").
- Košir, M. (2018). Vloga Slovenske vojske pri zagotavljanju kibernetске varnosti slovenske družbe: zaključna naloga. Ministry of Defence of the Republic of Slovenia. <http://dk.mors.si/IzpisGradiva.php?lang=slv&id=895>
- Levnik, M. (2024). Kibernetска varnost v luči digitalne transformacije in uporaba oboroženih sil: zaključna naloga. Ministry of Defence of the Republic of Slovenia. <http://dk.mors.si/IzpisGradiva.php?lang=slv&id=1497>
- Štrucl, D. (2020). Pravni in institucionalni vidiki ureditve kibernetске varnosti in obrambe Republike Slovenije: doktorska disertacija. University of Ljubljana.
- Zupančič, K. (2020). Analiza pravnega urejanja kibernetске varnosti v Sloveniji in EU: magistrsko delo. University of Ljubljana. <https://repozitorij.uni-lj.si/IzpisGradiva.php?lang=slv&id=124119>
- Ministry of Defence of the Republic of Slovenia. (2024). Adriatic Regional Cyber Cooperation Exercise (ARSC2EX 24) – Final Report. <https://www.gov.si/>
- Ministry of Defence of the Republic of Slovenia. (2020). Bela knjiga o obrambi Republike Slovenije (White Paper on Defence). <https://www.gov.si/assets/ministrstva/MO/Dokumenti/BK2020.pdf>

9.4 Annex 1 – In-depth interview questionnaire

Question 1:

From your perspective, how does cybersecurity technology transfer contribute to enhancing national security and resilience in [Country Name]? Could you provide examples of successful initiatives or highlight areas needing improvement?

Purpose:

This open-ended question encourages stakeholders to share detailed insights and specific examples, facilitating a deeper understanding of the practical implications and challenges of cybersecurity technology transfer within the national context.

Question 2:

In your opinion, how effectively the current national cybersecurity strategy has been implemented so far?

Question 3:

Which organisations play a pivotal role in your country's cybersecurity ecosystem, and how do they collaborate to address cybersecurity challenges?

Question 4:

What are the most pressing cybersecurity challenges facing your country, and what measures are being taken to address them?

Question 5:

How does your country engage in international cybersecurity cooperation, and what benefits or challenges have arisen from these partnerships?

Question 6:

How do you define technology transfer in the context of cybersecurity, and why is it important for your organization or sector?

Question 7:

Can you elaborate on the legal and regulatory frameworks that facilitate or hinder cybersecurity technology transfer in your country?

Question 8:

Which national institutions are most actively involved in cybersecurity technology transfer, and how do they collaborate to facilitate this process?

Question 9:

What are the primary incentives your organization faces in participating in cybersecurity technology transfer?

Question 10:

What are the primary barriers your organization faces in participating in cybersecurity technology transfer?

Question 11:

Can you share examples of successful cybersecurity technology transfer initiatives your organization has been involved in, and what factors contributed to their success?

Question 12:

Can you describe the national policies or frameworks in place for cybersecurity information sharing, and how effectively they function in practice?

Question 13:

Which platforms or tools does your organization use for sharing and receiving cybersecurity threat intelligence, and how effective are they?

Question 14:

Can you share experiences of international cooperation in cybersecurity information sharing that have benefited your organization?

Question 15:

What challenges has your organization faced in sharing cybersecurity information with partners from other sectors?

Question 16:

Does your organization engage in informal cybersecurity information sharing? If so, through which channels, and how valuable are these interactions?

Question 17:

How does your organization perceive the role of dual-use cybersecurity technologies in balancing national security and innovation?

Question 18:

Can you elaborate on the national policies or frameworks that regulate dual-use cybersecurity technologies, and how effectively they function in practice?

Question 19:

What challenges has your organization faced in regulating or managing dual-use cybersecurity technologies?

Question 20:

Can you share examples of cybersecurity technologies with dual-use applications your organization has developed or utilized, and what factors contributed to their dual-use nature?

9.5 Annex 2 – Online survey

Question 1:

Which sector do you represent?

- Public government
- Private sector
- Academic/ research Institution
- Civil society
- Military related organisation
- Other (please specify)

Question 2:

Which type of institution do you represent?

- Government agency
- Research institution
- Private sector company
- Non-Governmental Organization
- Military related organisation
- Other (please specify)

Question 3:

On a scale from 1 (Not Important) to 5 (Extremely Important), how important is international collaboration in cybersecurity for your organisation?

Purpose:

This Likert-scale question quantifies the perceived importance of international collaboration, allowing for statistical analysis across different stakeholder groups and countries.

Question 4:

On a scale of 1 (Not Effective) to 5 (Highly Effective), how would you rate the implementation of the national cybersecurity strategy in your country?

Question 5:

Which of the following areas do you consider to be the most significant challenges in your country's cybersecurity landscape? (Select up to three)

- Lack of skilled professionals
- Insufficient funding
- Inadequate legal frameworks
- Poor inter-agency coordination
- Limited public awareness
- Other (please specify)

Question 6:

To what extent does international cooperation enhance your country's cybersecurity capabilities?

- Not at all
- To a small extent
- To a moderate extent
- To a great extent
- To a very great extent

Question 7:

On a scale from 1 (Not Important) to 5 (Extremely Important), how important is technology transfer in advancing cybersecurity capabilities in your country?

Question 8:

How familiar are you with the national legal frameworks governing cybersecurity technology transfer?

- Not at all familiar
- Slightly familiar

- Moderately familiar
- Very familiar
- Extremely familiar

Question 9:

Which of the following factors act as barriers to cybersecurity technology transfer in your country? (Select all that apply)

- Lack of government funding programmes
- Lack of public-private partnerships
- Legal constraints
- Lack of trust among stakeholders
- Insufficient resources
- Technical incompatibilities
- Other (please specify)

Question 10:

Are you aware of any successful cybersecurity technology transfer initiatives in your country?

- Yes
- No
- If yes, please provide a brief description:

Question 11:

How familiar are you with your country's cybersecurity information-sharing policies and frameworks?

- Not at all familiar
- Slightly familiar
- Moderately familiar
- Very familiar
- Extremely familiar

Question 12:

Which of the following mechanisms does your organization utilize for cybersecurity threat intelligence sharing? (Select all that apply)

- National CERT
- ISACs

- Private threat intelligence platforms
- Informal networks
- Other (please specify)

Question 13:

Has your organization participated in international cybersecurity information-sharing initiatives?

- Yes
- No
- If yes, please specify

Question 14:

Which of the following challenges hinder cross-sectoral cybersecurity information sharing in your experience? (Select all that apply)

- Lack of trust between sectors
- Legal or regulatory barriers
- Technical incompatibilities
- Insufficient resources
- Other (please specify)

Question 15:

Which informal channels does your organization use for cybersecurity information sharing? (Select all that apply)

- Professional associations
- Industry conferences
- Social media platforms
- Personal networks
- Other (please specify)

Question 16:

On a scale from 1 (Not Important) to 5 (Extremely Important), how important are dual-use cybersecurity technologies to your organization's operations?

Question 17:

How familiar are you with your country's policies and frameworks governing dual-use cybersecurity technologies?

- Not at all familiar
- Slightly familiar
- Moderately familiar
- Very familiar
- Extremely familiar

Question 18:

Which of the following challenges hinder effective regulation and management of dual-use cybersecurity technologies in your experience? (Select all that apply)

- Legal or regulatory barriers
- Ethical considerations
- Technological complexities
- Lack of international cooperation
- Other (please specify)

Question 19:

Are you aware of any cybersecurity technologies with dual-use applications in your country?"

- Yes
- No
- If yes, please provide a brief description (open answer)

9.6 Annex 3 – Questions to guide the national validation workshops

Question 1:

Considering the preliminary findings on the national cybersecurity landscape, do you agree with the identified strengths and gaps in technology transfer and information sharing mechanisms? What additional factors or perspectives should be considered to provide a more comprehensive understanding?

Purpose:

This prompt fosters interactive discussion among experts, validating the initial findings and uncovering additional insights or overlooked aspects, thereby enhancing the robustness of the case study.

Question 2:

Based on the preliminary findings, do you agree with the assessment of the national cybersecurity strategy's effectiveness and areas for improvement? What additional insights can you provide?

Question 3:

Are there any key stakeholders or collaborative initiatives in the national cybersecurity landscape that have been overlooked in our preliminary analysis?

Question 4:

Do you concur with the identified challenges and gaps in the national cybersecurity framework? Are there additional issues that should be considered?

Question 5:

Are there specific international partnerships or cooperative efforts that have significantly influenced your country's cybersecurity posture? What lessons can be drawn from these experiences?

Question 6:

Do you agree with the defined concept and importance of technology transfer in cybersecurity as presented? Are there additional aspects or perspectives that should be considered?

Question 7:

Are there any legal or regulatory barriers that significantly impact the effectiveness of technology transfer in your country?

Question 8:

Are there any key institutions or collaborative initiatives in the national cybersecurity technology transfer landscape that have been overlooked in our preliminary analysis?

Question 9:

Do you agree with the identified incentives and barriers to cybersecurity technology transfer? Are there additional factors that should be considered?

Question 10:

Based on our findings, are there additional successful cybersecurity technology transfer initiatives that should be highlighted? What lessons can be drawn from these examples?

Question 11:

Are the current national policies and frameworks sufficient to facilitate effective cybersecurity information sharing? What improvements would you suggest?

Question 12:

Are the current threat intelligence sharing mechanisms and tools adequate for your organization's needs? What enhancements would you recommend?

Question 13:

What international best practices in cybersecurity information sharing could be adopted or adapted to improve national mechanisms?

Question 14:

What strategies can be implemented to overcome the identified challenges in cross-sectoral information sharing?

Question 15:

How can informal information-sharing practices be integrated or aligned with formal mechanisms to enhance overall cybersecurity resilience?

Question 16:

Do you agree with the defined concept and importance of dual-use cybersecurity technologies as presented? Are there additional aspects or perspectives that should be considered?

Question 17:

Are the current national policies and frameworks sufficient to manage dual-use cybersecurity technologies effectively? What improvements would you suggest?

Question 18:

What strategies can be implemented to overcome the identified challenges in regulating and managing dual-use cybersecurity technologies?

Question 19:

Based on our findings, are there additional cybersecurity technologies with dual-use applications that should be highlighted? What lessons can be drawn from these examples?