ACTION PLAN

Chamber of Commerce and Industry of Slovenia

CYBER
Interreg Europe

European Union
European Regional
Development Fund

INTRODUCTION

At a time of an evolving landscape of threats, cybersecurity's place at the top of the EU's political agenda raises no doubts. Since its first ever cybersecurity strategy adopted in 2013, the EU has adopted and initiated a number of policy measures to strengthen its cybersecurity capabilities and resilience against cyberattacks: NIS Directive, Digital Single Market Strategy, the proposal to create the European Cybersecurity Competence Centre and Network, the EU Cybersecurity Act, as well as the Digital Europe and the Horizon Europe programmes.

The current EU policies suggest that in the context of cybersecurity, the core players are Member States' national governments, supported by dedicated EU bodies, such as the European Union Agency for Cybersecurity (ENISA). However, because of its multifaceted and all-encompassing nature, cybersecurity policy requires a diversification of the actors involved in its implementation. On one hand, ensuring a close cooperation with the private sector has been recognised as an important step in strengthening the EU's cybersecurity, resulting in the contractual public-private partnership on cybersecurity signed with the European Cyber Security Organisation (ECSO) in 2016. But on the other hand, European regions have often lacked recognition as important cybersecurity actors.

Uniquely positioned, regions hold a privileged connection to their local ecosystems. They have the biggest potential to connect technology with end users, to assist local small and medium enterprises (SMEs), and to provide them with business support and access to innovative technologies. Regions can significantly contribute to the development and deployment of European cybersecurity products and services, thus reducing the EU's reliance on solutions coming from third countries and non-European providers. In the near future, the EU cybersecurity landscape will be shaped by initiatives having a direct impact on regional ecosystems, such as the European Cybersecurity Competence Centre and Network, the European digital innovation hubs and renewed smart specialization strategy in each region. Interregional cooperation is therefore key to identifying solutions and moving towards a more integrated cybersecurity market.

The **CYBER project** has been initiated under the EU Interreg Europe programme and the European Regional Development Fund (ERDF) financial instrument to strengthen the local cybersecurity SMEs and to boost interactions among the European regional cybersecurity ecosystems. The lack of cooperation among different cybersecurity stakeholders and different ecosystems is identified as one of the challenges preventing local cybersecurity SMEs from scaling up and internationalising their business. To address this challenge, project partners work together through a series of interregional events to develop and implement regional action plans and concrete policy instruments.

The CYBER involves nine institutional partners, representing different EU countries and regions:

- **Bretagne Development Innovation agency (France),**
- **Institute for Business Competitiveness of Castilla y León (Spain),**
- **Tuscan Region (Italy),**
- **Digital Wallonia agency (Belgium),**
- **Brittany Region (France),**
- **Kosice IT Valley (Slovakia),**
- **Chamber of Commerce and Industry of Slovenia (Slovenia),**
- **Estonian Information System Authority (Estonia),**
- **the European Cyber Security Organisation (Belgium).**

CYBER overall objective is to boost competitiveness of cybersecurity SMEs, thanks to improved public policies. It involves public authorities that can help knock down barriers of market fragmentation, lack of coordination of regional actors and lack of skills. Medium-term aim is to ensure greater coherence between offer and market demand, with a chance to build up skills and merge competences. In the long term, by making the digital world safer, the CYBER initiative contributes to the development of the EU digital market.

During its first phase, CYBER focused on identifying main barriers: lack of coordination between relevant actors, market fragmentation and lack of skills. For each barrier, regional strengths, weaknesses, opportunities and threats were identified, using SWOT analysis. The aim was to identify characteristics and key services that an innovation ecosystem supporting SMEs in the cybersecurity sector should deliver. Based on their level of cyber-development, CYBER partners also identified good practices that represent strengths of their territories and potential solutions to other partners' needs. These good practices fall under two different groups of policy measures: those that support the structure of the cyber innovation ecosystem and those that support advanced services provided within the ecosystem (such as labels, access to public and private funding, capacity building etc.). As a result of this interregional exchange process, good practices and solutions have been selected by partners in a perspective of transfer and adaptation and have been collected into **regional Action Plans**. These Actions Plans represent, for concerned regional authorities, a concrete road map for designing and targeting more and better funding to increase competitiveness of cybersecurity SMEs. Their relevance is also crucial within an EU context, as they provide inputs that can contribute to the European Investment for Growth and Jobs programme and the European Territorial Cooperation programme, as well as to address cybersecurity challenges through the newly proposed NIS2 Directive lenses. Produced by CYBER partners, these Actions Plans are therefore key documents both for regional cooperation across Europe and for policymaking at the EU level.

GENERAL INFORMATION

Name of the project: CYBER
Partner organisation: Chamber of Commerce and Industry of Slovenia
Country: Slovenia
NUTS2 region: Western Slovenia

Contact person:

Željka Kelkedi
zeljka.kelkedi@gzs.si
+386 1 5898 104

Grit Ackermann
grit.ackermann@gzs.si
+386 1 5898 418

POLICY CONTEXT

The Action Plan aims to impact:

- Investment for Growth and Jobs programme
- European Territorial Cooperation programme
- *Other regional development policy instrument*

Name of the policy instrument addressed:
Strategy for Cybersecurity of Slovenia

DETAILS OF THE ACTIONS ENVISAGED

ACTION 1: Promote Innovative and R&D-Based Cybersecurity SMEs in the Renewed Cybersecurity Strategy of Slovenia and its Related Action Plan

The background - ***territorial need/policy context***

The Government Information Security Office (URSIV), which succeeded the Information Security Administration of the Republic of Slovenia (operating from 2019 as a new agency established by the then competent Managing Authority – Ministry of Public Administration of the Republic of Slovenia (MJU)), was established on 20 July 2021 and became operational on 31 July 2021. URSIV is the competent national authority in the field of information and cybersecurity. Its core mission is to increase resilience to cyberthreats that can threaten individuals, businesses, the government, and society at large.

URSIV has the task to renew the Cybersecurity Strategy of Slovenia and prepare a related action plan for the realisation of the strategy. The original Cybersecurity Strategy of Slovenia only insufficiently addressed the needs of cybersecurity SMEs and did not set any objectives related to strengthening this sector. An action plan that would specify adequate measures and actions to reach the strategy's objectives had not been accepted at the time. Consequently, no actions were planned or implemented to support the private cybersecurity sector, even though the original strategy had recognised the need to develop CS services and products in Slovenia.

The government institutions, especially URSIV, recognised the lack of cooperation with the private sector as a shortcoming of the original strategy. Market fragmentation and the lack of a skilled workforce in cybersecurity are significant challenges for the cybersecurity business community in Slovenia. A shrinking of this sector or a decrease in competitiveness would have negative consequences for the digital transformation of Slovenian society, the critical infrastructure, and the business community, as well as for the country itself.

Also related to recognising this shortcoming of the original strategy by URSIV was a proactive approach towards cybersecurity companies and an invitation to the CCIS's Cybersecurity Working Group to engage the private sector in drafting the renewed Cybersecurity Strategy of Slovenia and the related Action Plan.

The CYBER project was more than welcome to tackle this shortcoming, foster the cooperation of different actors in the cyber ecosystem, and set goals related to the development of cybersecurity skills and competences, as well as increasing the competitiveness of cybersecurity SMEs.

Estonia is a dedicated digital society with a very stimulative and start-up and business-friendly support environment. Embedded in this existing support structure is the support available for cyber SMEs. It can serve as a role model for Slovenia. The Cybersecurity Strategy of Estonia served as an example of good practice. We also learned from other partners about successful measures for creating a nurturing ecosystem for cyber SMEs, namely in Tuscany and Brittany. From Tuscany, we learned about the educational programme for cyber experts. In contrast, from Brittany, we learned about cyber competitions as a tool for working with the cybersecurity community and creating informal learning and networking opportunities. The good practices were discussed with the LOCKS group in order to adapt them to the Slovenian environment and included in our recommendations for the action plan accompanying the new Cybersecurity Strategy of Slovenia.

These are ***the main learning processes***:

- We learned about the Estonian strategy at the partner meeting in Tallin and later during other (online) partner meetings
- During an online meeting with the Estonian partner, on 1 June 2020, we had a bilateral exchange to learn more about the strategy, its related programme, and the implementing body,
- In October 2020, we organised the first CCIS CYBER Night, which was a great success. After organising the CYBER Night in Slovenia with the support of the BDI, we recognised the importance of such events for informal learning opportunities, exchange and cooperation and for the cybersecurity community in general and decided to integrate cyber competitions into our action plan.
- Webinar organised by CYBER with an Estonian expert in student competitions in autumn 2020
- A meeting took place with Enterprise Estonia in January 2021 to learn more about the public-private partnerships in supporting cybersecurity SMEs
- Meeting with RIA and Estonia Enterprise in May 2021 with Estonian partners and our MA (at that time Information Security Administration of the Republic of Slovenia) to clarify additional questions regarding the Estonian Cybersecurity Strategy and its implementation.

The action

We prepared two policy recommendations:

A) ***Policy recommendation for the strategy***: Support the managing authority in the renewal of the cybersecurity strategy and addressing the needs of innovative and R&D based cybersecurity SMEs

B) ***Policy recommendation for an action plan***: Support the managing authority in preparing an action plan related to Slovenia's cybersecurity strategy and defining actions and measures addressing the needs of innovative and R&D based cybersecurity SMEs

Aims formulated:

- Increasing the competitiveness of the cybersecurity sector in Slovenia
- Fostering the development of cybersecurity within the business community
- Strengthening the development of human resources in cybersecurity

Actions (to be) implemented:

Before the foundation of the Government Information Security Office (URSIV), we worked with the then responsible governmental organisations, which were the Ministry of Public Administration (MJU), the Government Office for the Protection of Classified Information (UVTP) and Information Security Administration of the Republic of Slovenia. Representatives of all organisations participated in LOCKS activities.

The first activities with the LOCKS group included a thematic workshop with key actors preparing a SWOT analysis on the ecosystem for cybersecurity SMEs in Slovenia (16 November 2019) at the CCIS.

Shortly after the establishment of Information Security Administration in December 2019, there was a meeting (on 11 February 2020) with the appointed director of the Administration, CCIS representatives and CYBER project manager, as well as the LOCKS group leader. At this meeting, it was agreed that the CCIS (Committee for Cybersecurity) and the CYBER project coordinate a consultation process with the cybersecurity (business) community and cooperate with the Information Security Administration in the preparation of the renewed strategy and define measures for an action plan that would support the implementation of Slovenia's renewed cybersecurity strategy. The approval for the strategy and the respective action plan was planned for the end of 2020 but has now been postponed to 2021.

We started studying the Estonian cybersecurity strategy.

- February–June 2020: Online meeting with LOCKS members and other stakeholders to collect proposals for a policy recommendation, first focussed on the strategy
- LOCKS meeting (27 May 2020) to discuss the policy recommendations
- Bilateral online meeting with the partners from Estonia (1 June 2020) to learn more about the Estonian cybersecurity strategy and how they address actions to promote innovative and R&D based cybersecurity SMEs
- June 2020: Preparation of draft policy recommendations for the strategy; thereafter, we started working on measures for the action plan
- Information Security Administration organised a one-day design thinking workshop on the cybersecurity strategy (20 October 2020) for the expert community, to which the CCIS was also invited with five participants. Many members of the CYBER LOCKS group participated. The design thinking workshop covered the entire cybersecurity strategy, but included many areas relevant in the context of competitiveness of cybersecurity SMEs/CYBER project:

    ○ Human resource development,
    ○ Research and Development,
    ○ Cooperation of public and private sector in assuring cybersecurity,
    ○ Raising awareness and know-how on cybersecurity among the general public and the business community.

An evaluation of the current measures in these four areas was performed at the DT workshop, along with an assessment of the draft measures proposed for the new strategy. It can be said that this workshop changed the stakeholders' views on the need for HR development. The following were recognised:

- How crucial the constant support to the development of cybersecurity competences is, both in formal as well as in informal education and training or career paths;
- The need to improve cooperation with the private sector (public-private partnership) and support to SMEs working in cybersecurity.

Another important contribution was the communication activities of the Slovenian CYBER team focussed on raising awareness among the business community of the importance of the cybersecurity strategy and action plan (LOCKS events with members of the expert community invited, newspaper articles, conference contribution) during the time of drafting the policy recommendations.

- After working further on the measures to be proposed in the action plan, on 6 January 2021, there was a meeting of the key LOCKS group members to confirm the final proposals for the strategy and the action plan.
- 13 January 2021: a more comprehensive document with policy recommendations for both the strategy and for the action plan was sent to Information Security Administration for feedback
- Web meeting for representatives of the Information Security Administration, the MJU, the CYBER team and RIA and Enterprise Estonia to discuss open questions on the Estonian Cybersecurity Strategy and its implementation.

The steps ahead of us are:

- Further work on the recommendations in cooperation with LOCKS and the MA
- Final consultation with the MA on the recommendations
- Due to the activities of the EU Council presidency, it is expected that the MA will publish the strategy and action plan in 2022
- The CCIS will continue communication with the MA and LOCKS members and monitor the process of implementation. Although the strategy and action plan are not yet published, URSIV and other involved actors

(including the CCIS) have started working on projects and measures from the action plan.

The cybersecurity sector is dominated by SMEs. Strengthening the competitiveness of these SMEs is essential for cybersecurity in Slovenia. The main policy change proposed by CYBER is to create a support environment for cybersecurity SMEs in Slovenia that addresses their needs. The main challenge for cybersecurity SMEs is the lack of skilled staff. Access to R&D programmes or R&D programmes offering long-term orientation and involvement of SMEs in the development of the cybersecurity sector is another feature that has been missing. The public sector has paid too little attention to the involvement of SMEs in cybersecurity projects.

The **main recommendations** to be included in the national Action Plan of the renewed Cybersecurity Strategy of Slovenia are as follows:

1. Addressing the needs of companies in the cybersecurity sector in the Strategy and the related national action plan (improving the competitiveness of SMEs in the cybersecurity sector) through:

- HR development, as well as talent and employee retention, which is crucial for the development of the field – active promotion of HR development through national policy measures, especially in the design and establishment of educational programmes and certification of individuals
- Project-based promotion of cybersecurity as a career opportunity among students, such as the annual youth CYBER Night competition (organised by the Chamber of Commerce and Industry of Slovenia), as preparation for participation in the European Cyber Security Challenge (ECSC), and participation in international cyber defence exercises - Locked Shield
- Establishment and coordination of a national R&D cybersecurity programme
- Investments in cybersecurity research and development projects, multi-stakeholder projects, synergies with EU tenders and national needs.

2. An awareness-raising programme for business leaders on cyber threats and raising the security culture.

3. Acceleration of the application of vouchers for knowledge development, and verification of cybersecurity measures and certification, as well as expansion of the scope of the cybersecurity voucher.

None of these recommendations listed above was addressed in the previous strategy. The renewed Cybersecurity Strategy of Slovenia and its Action Plan will point out the importance of a support environment for the cybersecurity SMEs to enhance their competitiveness. The documents will address the lack of cybersecurity specialists in general and in SMEs and will present actions to promote the profession as a career option. Cybersecurity and, in particular the care for critical infrastructure, relies on close cooperation between the public and private sectors, civil society and academia. The Slovenian strategy will recognise the importance of promoting the development of businesses and public-private partnerships and projects involving SMEs in the cybersecurity sector, which are vital for a modern digital economy since only growing and innovative cybersecurity companies can provide leading technologies, training and advice to businesses and government bodies.

Players involved

The managing authority (since July 2021) is the Government Information Security Office (URSIV), preceded by the Information Security Administration of the Republic of Slovenia, i. e. the Ministry of Public Administration (MJU) and the Government Office for the Protection of Classified Information (UVTP). URSIV is the competent national authority in the field of information and cybersecurity and as such it handles and cooperates in all cyber- and information security activities in Slovenia.

Representatives of all the above-mentioned organisations participated in LOCKS activities throughout the duration of the project. The contact person from the MJU now works at URSIV, so there has been continuity in the cooperation.

Our chamber has established a Committee for Cybersecurity as a part of the Association of Informatics and Telecommunications (ZIT) in 2016. It is composed of representatives from companies in the cybersecurity branch (large companies and SMEs), academia (universities and research institutions) and governmental representatives. The Committee for Cybersecurity collaborates effectively with the national DIH and IKT Hm (national ICT cluster), which are part of the ZIT. The committee debates relevant issues on cybersecurity and takes action related to areas of common interest. The CYBER project was implemented in close cooperation with this committee, and it can be said that CYBER increased the committee's awareness of the relevance of cybersecurity SMEs for Slovenia's cyber ecosystem and the necessity to support them systematically.

Timeframe

The first draft of the policy recommendations both for the strategy and the action plan for the Information Security Administration – before the summer break 2020.

- January 2021 – more comprehensive policy recommendations provided to the Information Security Administration.
- Autumn 2021 – final policy recommendation document submitted to URSIV.
- URSIV publishes the renewed strategy and its action plan – expected for 2022.
- 2021–2023 – monitoring how our proposed policy recommendations (strategy) and measures (action plan) are being implemented/supporting their implementation.

Cost

Once the strategy and its related action plan are prepared, we can assess how much funding will be available to realise our proposed policy recommendations and action plan measures.

Funding sources

- Funding from EU funds
- National funding
- Funding from other stakeholders (including CCIS)
- Private sources (companies)

Monitoring and indicators

General indicators to monitor:

- Number of policy recommendations implemented in the strategy and the action plan
- the KPI of the cybersecurity sector as
  - the number of cybersecurity SMEs, end of 222 compared to 2017 (the year before the project started)
  - the number of employees in cybersecurity SMEs, end of 2022 compared to 2017 (the year before the project started)

Specific indicators

One key recommendation was to improve the cooperation between the private (SMEs) and the public sector; thus, we monitor the level of cooperation between the private and the public sector measured in the number of events or cooperation activities and investments. The data is collected by our chamber ICT cluster.

- Number of public-private cooperation activities and partnerships, measures in 2020, 2021 and 2022

One proposed measure is the organisation of hackathons and cybersecurity competitions on the national level and participation in European or international cybersecurity competitions. These competitions are an excellent informal learning opportunity, increase interest in cybersecurity and offer students the opportunity to meet and collaborate with cyber experts and firms. We propose the following monitoring:

- Number of competitions/hackathons/CYBER Nights organised: one competition per year, a total of two between 05/ 2021 – 04/2023
- Number of participants in the events: total: cca. 50 per year, a total of 100 between 05/ 2021 – 04/2023
- Number of participants in international or European competitions: 25 per year, a total of 50 between 05/ 2021 – 04/2023.

Date

Signature

Stamp of the organisation

CYBER

REPUBLIC OF SLOVENIA
GOVERNMENT INFORMATION SECURITY OFFICE

Šmartinska cesta 152, 1000 Ljubljana, Slovenia

T: 01 478 4778
E: gp.uiv@gov.si
W: http://www.uiv.gov.si/en/
Twitter: @URSIV_Slovenia

Letter of Endorsement

The Government Information Security Office (URSIV) is the National Competent Authority in the field of information and cyber security. It is the Managing Authority of the National Cybersecurity Strategy and its related Action Plan. URSIV expressed all the support to the Chamber of Commerce and Industry as CYBER project partner and has been member of the Local Group of Stakeholders.
We had the opportunity to participate in the meetings of the group, two interregional events and one staff exchange (all virtual) and other project activities such as the CYBER conference and the CYBER Night in Slovenia.

In these contexts, it was possible to follow and participate in the development of the project and to be aware of the quality of the work developed. CYBER will be an important contribution to the preparation of the National Cybersecurity Strategy. The CYBER Action Plan brings together the contributions of all the stakeholders involved and constitutes a valuable input for the development of the National Cybersecurity Strategy.

In this context, we endorse the CYBER Action Plan submitted by the Chamber of Commerce and Industry of Slovenia in the context of the Interreg Europe project CYBER.

Ljubljana, 23/8/2021

Sincerely,

Dr Uroš Svete
Acting Director
Government Information Security Office

REPUBLIKA SLOVENIJA
URAD VLADE RS ZA INFORMACIJSKO VARNOST
01
Ljubljana