



# Cybersecurity skills strategy Slovenia.

Final version.



Co-funded by  
the European Union

## About CyberHubs

The European Network of Cybersecurity Skills Hubs (CyberHubs) is a 3-year project aiming to enhance the cybersecurity skills ecosystem in Europe. It will establish a network of seven Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon and the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem.

[info@cyberhubs.eu](mailto:info@cyberhubs.eu) | [cyberhubs.eu](https://cyberhubs.eu)

## Project consortium

The CyberHubs consortium brings together 21 full partners spanning 11 European Member States and 3 associated partners.

### Full partners

[DIGITALEUROPE](#) | [ADECCO FORMAZIONE SRL](#) | [AGORIA](#) | [AMETIC](#) | [Athens University of Economics and Business](#) | [Breyer Publico SL](#) | [Cyber Ireland](#) | [EIT Digital](#) | [GZS/CCIS](#) | [HOWEST](#) | [INFOBALT](#) | [ITL Estonia](#) | [IVSZ](#) | [Kaunas University of Technology](#) | [NUMEUM](#) | [SEPE](#) | [Solvay Brussels School of Economics and Management](#) | [Tallinn University of Technology](#) | [Universidad Internacional de La Rioja \(UNIR\)](#) | [Ludovika University of Public Service \(NKE\)](#) | [UNIVERZA V MARIBORU](#)

### Associated partners

[Association of Applied Research in IT \(AAVIT\)](#) | [Digital Technology Skills \(DTSL\)](#) | [IT Ukraine](#)

## Legal Disclaimer

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 Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



**Co-funded by  
the European Union**

Copyright © 2024 by CyberHubs All rights reserved.

The project resources contained herein are publicly available under the [Creative Commons license 4.0 B.Y.](#)

## Cybersecurity skills strategy Slovenia, 2025, FINAL version.

Deliverable D.2.3 “Country-specific cybersecurity skills strategies”

Authors: Ines Vlahović (CCIS), Mateja Pucihar Baebler (ZIT), Andreja Lampe (CCIS), Muhamed Turkanović (UM FERI), Nika Jeršič (UM FERI)

Editors/Reviewers: Viktorija Batin (IVSZ), Jonas Čeponis (KTU)

Revision History			
Version	Date	Modified by	Version
0.1	24/12/2024	Ines Vlahović (CCIS), Mateja Pucihar Baebler (CCIS), Muhamed Turkanović (UM FERI), Nika Jeršič (UM FERI)	Draft version
0.2	27/12/2024	Ines Vlahović (CCIS), Andreja Lampe (CCIS)	Ready for a review
0.3	09/01/2025	Viktorija Batin (IVSZ)	Review
0.4	12/01/2025	Ines Vlahović (CCIS), Nika Jeršič (UM FERI)	Updates based on the feedback
0.5	17/01/2025	Jonas Čeponis (KTU)	Final review
0.6	24/01/2025	Ines Vlahović (CCIS), Nika Jeršič (UM FERI)	Updates based on the feedback
1	28/01/2025	Ines Vlahović (CCIS)	Initial published version

# Table of contents

1	Executive Summary .....	6
2	Introduction .....	8
2.1	Cybersecurity in Slovenia .....	8
2.2	Global and Regional Trends in Cybersecurity .....	8
2.3	Vision .....	9
3	Current Situation and Strategic Objectives .....	10
3.1	Key Actors in Cybersecurity Area .....	10
3.2	ECSF common language for Cybersecurity professional workforce development .....	12
3.3	EU and National Legal Regulations .....	12
3.4	Industry/Country Needs .....	13
3.5	Educational Landscape .....	13
3.6	Cybersecurity Skills Gap Assessment .....	14
3.7	Strategic Goals .....	14
3.7.1	Short-term Strategic Goals (Next 2 Years) .....	14
3.7.2	Medium-term Strategic Goals (3-5 Years) .....	15
3.7.3	Long-term Strategic Goals (>5 Years) .....	15
3.8	Conclusions .....	16
4	Action Plan .....	17
4.1	Initiative 1: Raise awareness for Cybersecurity profession/professional career opportunities .....	17
4.2	Initiative 2: Expand education and training programs/offerings .....	17
4.3	Initiative 3: Promote lifelong learning .....	18
4.4	Initiative 4: Innovation, Research & Development and Knowledge sharing .....	18
4.5	Conclusions .....	18
5	Evaluation and Monitoring .....	19
5.1	Metrics and Monitoring .....	19
5.2	Continuous Improvement .....	20
5.3	Conclusions .....	21
6	Conclusions .....	22
7	References .....	24

## List of Tables

Table 1: Potential KPIs for each initiative. ....	20
---	----

## List of Figures

Figure 1: List of key actors in Slovenia's cybersecurity domain. ....	11
Figure 2: CyberHub Slovenia Key Pillars of Skills Development .....	22

# 1 Executive Summary

## Introduction

This document outlines Slovenia's Cybersecurity Skills Strategy, designed to address the critical need for a skilled workforce capable of mitigating increasing cyber threats. It emphasizes the importance of bridging skills gaps, enhancing education, and fostering workforce preparedness to meet the demands of a rapidly evolving digital landscape. By promoting collaboration between academia, government, and industry, the strategy aims to establish a robust and sustainable cybersecurity ecosystem that enhances national resilience, safeguards critical infrastructure, and aligns with Slovenia's digital transformation goals.

## Objective

The aim of this document is to present a comprehensive strategy for developing Slovenia's cybersecurity workforce to address current and future challenges in the digital domain. It targets a diverse range of groups, including:

- **Students:** Encouraging early exposure to computer science and cybersecurity concepts.
- **Professionals:** Providing advanced training to enhance and renew qualifications.
- **Public and private sector employees:** Supporting organisations in meeting legal and operational cybersecurity requirements.
- **The public:** Raising awareness of cyber hygiene and the importance of cybersecurity.

Key areas of focus include integrating cybersecurity into educational curricula, implementing professional development programs, supporting lifelong learning, and conducting awareness campaigns. The strategy also seeks to position Slovenia's CyberHub as a leader in cybersecurity upskilling and reskilling efforts.

## Approach

The development of this strategy employs a mixed-methods approach, combining data-driven insights and collaborative frameworks to address Slovenia's cybersecurity skills landscape effectively. Key components include:

- **Local stakeholder engagement:** Actively involving educational institutions, industry experts, and government bodies.
- **Alignment with EU initiatives:** Ensuring compliance with the EU Cybersecurity Strategy, the NIS2 Directive, and the Digital Education Action Plan, while addressing unique national needs.
- **Participation in the CyberHubs project:** Leveraging the European network of cybersecurity skills hubs to foster international collaboration and the exchange of best practices.
- **Data-driven insights:** Grounding the strategy in findings from the "D2.1 Cybersecurity Skills Needs Analysis" document, which draws on surveys, labour market studies, and expert panel discussions to evaluate existing challenges and predict future needs.

By adopting this comprehensive approach, the strategy ensures alignment with national and EU directives while addressing Slovenia's specific cybersecurity skills challenges.

## Results

The document identifies critical gaps in Slovenia's cybersecurity skills ecosystem, including:

- A shortage of incident responders and cybersecurity practitioners.
- Limited educational programs that predominantly focus on technical skills, with insufficient emphasis on soft skills and practical application.

- Recommendations to expand training programs, address AI-related cybersecurity challenges, and foster public-private partnerships to enhance education and workforce readiness.

These findings underline the urgent need for targeted initiatives to build a skilled and resilient cybersecurity workforce capable of addressing Slovenia's growing cyber threats.

## Conclusions

The analysis highlights the pressing need to bridge the cybersecurity skills gap in Slovenia. Key takeaways include:

- The importance of integrating cybersecurity education at all levels, from foundational learning to advanced professional certifications.
- The need to strengthen public-private partnerships to align training initiatives with industry requirements and promote innovation.
- Raising public awareness of cybersecurity to embed it as a societal norm.

By addressing these priorities, the strategy provides a clear roadmap for enhancing Slovenia's cybersecurity capabilities, ensuring preparedness against evolving cyber threats, and supporting national and EU goals for digital transformation.

## 2 Introduction

### 2.1 Cybersecurity in Slovenia

Slovenia faces a significant shortage of skilled cybersecurity professionals, with analyses showing that the country is behind European standards in this critical field. The lack of experts is compounded by limited advanced training programs and by heavy reliance on upskilling internal employees within organisations, primarily focusing on technical skills. Cybersecurity education is not widely integrated into primary and secondary school curricula, and where it is available, the focus is predominantly on technical skills rather than the equally important soft skills and organisational aspects. This skills gap has resulted in a high demand for key roles such as incident responders and cybersecurity implementers, which are crucial for addressing the growing challenges in the country's cybersecurity landscape.

### 2.2 Global and Regional Trends in Cybersecurity

Slovenia is facing a growing wave of cyber threats as reported by Slovenian Computer Emergency Response Team (SI-CERT) each year. In 2023 alone, the reported financial impact of cybercrime in Slovenia reached € 55 million (1), with predictions estimating this figure will climb to € 72 million by 2025 (using Cybersecurity Venture prediction of 15% growth (2)). Globally, ransomware attacks rose by 73% in 2023 (3), with one cyber-attack occurring every 39 seconds (4). These alarming trends emphasize the urgent need to strengthen cybersecurity readiness across all sectors.

Slovenia's most vulnerable sectors include:

- **Healthcare:** Highly susceptible due to reliance on digital systems and underinvestment in cybersecurity.
- **Finance:** Faces risks from sensitive financial data and increasing use of digital banking.
- **Critical Infrastructure:** A prime target due to its essential role and potential for widespread disruption.

The rise of **Artificial Intelligence (AI)** is reshaping both the attack and defence sides of cybersecurity. Cybercriminals are leveraging AI to create more sophisticated phishing campaigns, automate vulnerability scanning, and develop advanced ransomware techniques. On the defence side, AI is becoming a critical tool for threat detection, automated incident response, and predictive risk assessment. These emerging technologies, while offering immense potential, also highlight the need for a more skilled cybersecurity workforce capable of managing and utilizing these advanced tools effectively.

The **NIS2 Directive** will play a pivotal role in shaping Slovenia's cybersecurity landscape. This regulation introduces stricter security requirements, risk management obligations, and enhanced reporting standards for operators of essential services and digital infrastructure. As a result, the demand for skilled cybersecurity professionals will significantly increase, as organisations must adapt to meet these new expectations.

Slovenia's National Cybersecurity Strategy from 2016 outlined commendable goals for improving cybersecurity awareness, resilience, and education, which align closely with the vision and objectives of the CyberHub skills strategy. However, progress has been limited due to limited investment and resource allocation. For example, Slovenia remains the only EU country without a dedicated computer science program in primary schools, a gap that reflects the broader challenges in building foundational digital literacy and cybersecurity awareness. The Chamber of Commerce and Industry prepared a declaration, where its members made a call on the Government of the Republic of Slovenia to take a decision on the introduction of a compulsory basic skills course in the first half of 2025, including cybersecurity, in primary and secondary schools and by 2028, establish and expand specialised degree and master's programs in universities with cybersecurity.

The combined impact of regulatory pressures, the global surge in cyber threats, and the adoption of AI and other emerging technologies will further intensify the need for a well-trained cybersecurity workforce. These challenges underscore Slovenia's urgent need to close its cybersecurity skills gap by investing in targeted education, fostering innovation, and building a more robust cybersecurity ecosystem to protect critical sectors and ensure a resilient digital economy.

## 2.3 Vision

Our **vision** is grounded in the belief that cybersecurity is the backbone of the modern economy and society:

*"We envision a future where CyberHub Slovenia  
leads the way in cybersecurity skills,  
through inclusive collaboration platform  
to build a resilient, innovative, and secure digital landscape."*

Through bold and coordinated efforts, innovative and timely activities, Slovenian CyberHub with/together its stakeholders/community will aim/aspire to position Slovenia as a hub of excellence in cybersecurity education, where cutting-edge knowledge and skills meet the current and future demands in rapidly evolving digital world. Through bold and coordinated efforts, innovative and timely activities, Slovenian CyberHub together with its stakeholders/community will aim to position Slovenia as a hub of excellence in cybersecurity education, where cutting-edge knowledge and skills meet the current and future demands of rapidly evolving digital world. CyberHub Slovenia will not only address current challenges but will also anticipate future threats by fostering a culture of continuous learning and innovation.

Slovenian CyberHub will act decisively to:

- Support the growing needs of the industry and public sector.
- Advocate for improvements in educational programs by showcasing global best practices and providing recommendations.
- Expand research and development capacities to position Slovenia as a leader in cybersecurity innovation.

## 3 Current Situation and Strategic Objectives

Current situation in Slovenia in the field of cybersecurity knowledge is based on the D2.1 Cybersecurity Skills Needs Analysis report. The report was developed using a mixed-methods approach, mainly it included the following activities:

- detailed desk research on demand and supply
- an analysis of job vacancies
- a comprehensive questionnaire
- insights gathered from experts by organizing the expert panel

Based on the above activities the following conclusions were made on the current situation:

- The growing need for skilled cybersecurity professionals, supported by targeted education and training initiatives are indicated. In the short term (next 2 years), the focus is on enhancing digital skills and increasing the number of cybersecurity professionals. In the medium term (3-5 years), the integration of cybersecurity into digital transformation and data-driven initiatives is crucial. In the long term (beyond 5 years), sustaining a robust cybersecurity ecosystem through continuous research, development, and strategic management will be essential.
- The range of available education programs in Slovenia is limited especially for those seeking in-depth expertise in specific areas of cybersecurity (where the demand is the highest).
- Only 27% of the postings are based in Slovenia and the trend is to focus on highly specialized roles.
- Based on the questionnaire a Cybersecurity Implementer/Expert and Incident responder are among the most sought-after roles. Followed by a Cybersecurity Auditor and Cyber Threat Intelligence Specialist, and Digital Forensics Investigator.
- Based on the questionnaire the following skills needs should be of a key priority for Slovenian companies: Cybersecurity skills, IT related skills, Organisation-related skills and Soft/transversal skills.
- During the expert panel several items were highlighted, which are also similar to other objectives: encourage a lifelong learning possibilities to remain adaptable in a rapidly evolving field; team leads to be educated in soft skills to effectively manage and lead expert teams; foster collaboration between industry and educational organisations to bridge knowledge gaps and prepare graduates for real-world challenges; a need for shorter and targeted trainings on niche topics, which enhances skill of the experts.

Overall, the Cybersecurity skills strategy for Slovenia aims to:

- bring together and form a long-term alliance of Slovenian key players in the field of cybersecurity, especially educational organisations, faculties, high schools, and companies to foster collaboration/cooperation and advancements on cybersecurity skills development.
- provide educational and training instruments that are updated regularly as a response to ongoing advancements in the field of cybersecurity (having in mind the integration of AI and the rise of the deep tech technologies) and the need of the workforce (in different levels of expertise).

Slovenia is experiencing a significant shortage in cybersecurity experts, especially in crucial roles such as Cybersecurity Implementer, Incident Responder, and Chief Information Security Officers. The demand is amplified by the enactment of the EU's NIS2 Directive, which mandates stricter cybersecurity measures across various industries.

### 3.1 Key Actors in Cybersecurity Area

The Slovenian CyberHub ecosystem is built on several important actors. ICT companies develop and maintain key cybersecurity technologies and services, while government entities regulate, fund and oversee national cybersecurity efforts to protect public systems. Policymakers establish frameworks and strategies to ensure security at national and organisational level. Educational institutions and research organisations provide the knowledge, training and innovation needed to advance the field. Students, as the future workforce, are acquiring the skills and knowledge needed to meet

the growing demand for cyber security professionals. Together, these actors form the backbone of a resilient and adaptive cybersecurity environment.

Slovenia's key actors in cybersecurity domain presented in Figure 1 include multiple government agencies, private companies, and academic institutions all of which are having a strong interest in minimizing the skills gap of current and future cybersecurity workforce.



Figure 1: List of key actors in Slovenia's cybersecurity domain.

## 3.2 ECSF common language for Cybersecurity professional workforce development

Cybersecurity Professional competences performance play a vital role for the European economy and society as a whole, and dedicated European reference frameworks that can be used by all key stakeholders of the digital professional eco-system are essential.

The European Cybersecurity Skills Framework (ECSF) published by ENISA in 2022<sup>1</sup>, being the result of joint work between ENISA and a dedicated AdHoc Work Group composed of Cybersecurity Professionals from many European countries, provides the needed common language and reference point for all parties to act upon, giving a common basis for specific and combined action for cybersecurity professional workforce development at all levels and across Europe in the short, mid and long-term.

The key objectives of the ECSF are:

- Establishing a common understanding of the most typical cybersecurity professional roles, missions and tasks required in the cyber secure organisation, together with their competences, skills and knowledge requirements, that can be used by and for individuals, organisations, learning providers, policy makers and cyber enthusiasts in all EU Member States, in order to effectively address the cybersecurity skills shortage.
- Contributing to further facilitate the recognition of cybersecurity professional-related skills and competences, the design of market needs oriented learning programmes, the cybersecurity workforce development in the organisation, and career guidance to individuals.

The 12 Cybersecurity Professional Role Profiles provided by the ECSF are ensuring the common language for the CyberHubs consortium across all work stages, and they are implemented from multiple viewpoints on European and national levels in workplace, learning, legal and policy making context. Adopting the ECSF as a high-level taken strategic decision significantly accelerates collaboration processes in the country and EU-level connected and from the start, enabling all cybersecurity eco-system key stakeholders to

- Get a **common understanding** of the necessary professional roles, competences, skills and knowledge,
- Support **cybersecurity workforce roles and skills needs identification, planning and development**, e.g. in order to prepare for organisational compliance with the new coming NIS2 Directive<sup>2</sup>,
- Facilitate **cybersecurity skills recognition**,
- Support the **design of cybersecurity related training programmes**,
- Help **shape content of applications for funding programmes** on national and European levels,

In this context, it is crucial to understand the ECSF as a flexible offer and as a tool that is provided for flexible usage. The framework seeks to enable wherever helpful and never to restrict. This can be easily achieved by selecting the components that are most suitable in context, and further customising where needed.<sup>3</sup>

## 3.3 EU and National Legal Regulations

The cybersecurity regulatory landscape in Slovenia is shaped by national and European legislation, creating essential requirements for cybersecurity practices. At the national level, key regulations include the Information Security Act

---

<sup>1</sup> [ECSF Part 1: 12 Cybersecurity Professional Role Profiles](#), ENISA 2022

<sup>2</sup> See ENISA Report “Preparing for NIS2 Compliance — NIS2 Mapping with ECSF Role Profiles” expected in 2025, reference to be added when available.

<sup>3</sup> See [ECSF Part 2: User Manual](#), ENISA, 2022

(ZInfV)(5) enacted in 2018, which provides a comprehensive framework for information security. Additionally, Slovenia follows the Personal Data Protection Act (ZVOP-2)(6), aligned with the GDPR, and the Electronic Communications Act (ZEKOM2)(7), which addresses cybersecurity aspects related to communications. At the EU level, Slovenia is working to integrate the NIS2 Directive, anticipated to increase the demand for cybersecurity roles and skills. The transposition of EU regulations often directly applies until national laws elaborate these directives to fit Slovenia's context.

#### Legal and regulatory framework

- **GDPR:** Imposes strict data protection standards, requiring expertise in secure personal data management, identifying and mitigating cybersecurity risks and effectively reporting breaches.
- **NIS2 Directive:** Strengthens security requirements, focusing on skills in risk management, implementation of advanced security measures and incident responding.
- **Cyber Resilience Act (CRA):** Necessitates professionals who understand secure software and hardware development and can conduct assessments and manage product lifecycle security.

### 3.4 Industry/Country Needs

The implementation of new regulations, such as the NIS2 directive, is anticipated to increase the demand for cybersecurity professionals, further widening the existing skills gap. Moreover, the growing prevalence of remote job postings and the acquisition of Slovenian ICT companies by foreign owners are intensifying the local talent shortage. The demand for skilled professionals already surpasses the available supply, and this disparity is projected to grow. Regulations like NIS2, coupled with the escalating frequency of cyber-attacks, are expected to amplify the need for cybersecurity experts, exacerbating the gap even further.

To address this challenge, a cybersecurity skills forecasting model will be used for a yearly update on cybersecurity skills needs, both in Slovenia and internationally. This model provides critical insights into which cybersecurity roles and skills are gaining importance, and which are becoming less critical. By combining quantitative data with qualitative analysis, this approach will help anticipate trends and inform strategies to bridge the skills gap. The results from the D2.2 deliverable on the forecasting model will also be incorporated to strengthen these efforts.

### 3.5 Educational Landscape

Slovenia's educational landscape for cybersecurity is evolving to address the increasing demand for skilled professionals in this critical field. But, despite the growing recognition of cybersecurity's importance, Slovenia faces several challenges in its educational sector:

1. **Limited program availability:** While some public and private institutions offer cybersecurity programs, the number of specialized courses is insufficient to meet the growing demand. Advanced topics are especially underrepresented.
2. **Focus on technical skills:** Current programs primarily emphasize technical skills, with less focus on organisational and soft skills that are essential for effective cybersecurity operations.
3. **Student engagement:** There's a decline in students enrolling in technical and IT fields, and high dropout rates further reduce the pool of qualified graduates.
4. **Industry collaboration needs:** While collaborations between universities and IT companies help students secure jobs, there is still a lack of central coordination among educational and industry stakeholders, which enhance training and workforce readiness.

Therefore, it is recommended to expand educational programs by introducing a more specialized training, including short-term, certification-based courses that align with industry needs. Soft skills development should be encouraged by integrating the topics into the cybersecurity programs to prepare professionals for effective collaboration and leadership roles.

## 3.6 Cybersecurity Skills Gap Assessment

Slovenia is struggling with two problems: a shortage of skilled people and the concern where these skills could be obtained. The Cybersecurity Skills Needs Analysis report (8) reflects a critical mismatch between industry needs and the available workforce's qualifications. The recommendation is to prioritize and focus on the most in-demand skills, ensuring the most critical areas are adequately covered.

The key skills to address are:

- **Cybersecurity skills:** Incident Management, Threat Analysis, Communications Security, Cloud Security, Information Systems & Network Security/Cyber Resiliency, Incident Management and Access Controls/ Identity Management, Data Privacy.
- **IT related skills:** System Administration & Integration, Data Analysis, Network Management, Software Development & Computer Languages, Enterprise Architecture & Infrastructure Design, Operating Systems, Testing and Evaluation and Database Administration.
- **Organisation-related skills:** Risk Management, Business Continuity, Process, Strategic Relationship Management and Strategic Planning.
- **Soft/transversal skills:** Problem-solving, Acting Responsibly, Acting Independently, Communication, Leadership, Collaborate in teams, Analytical thinking and Ethical Behaviour.

## 3.7 Strategic Goals

**Slovenian CyberHub aims to strengthen cybersecurity education through targeted initiatives that address current gaps and align with future needs.** These efforts will involve active collaboration with educational institutions, industry stakeholders, and policymakers to ensure current and future skilled workforce is capable of tackling evolving cyber threats.

### 3.7.1 Short-term Strategic Goals (Next 2 Years)

#### 3.7.1.1 Strategic Goal 1: Raise Awareness for Cybersecurity Careers

Promote cybersecurity careers by raising awareness of their importance and the opportunities they present as a viable career path.

Key Activities:

- Launch campaigns to target children, students, job seekers, and professionals to promote cybersecurity professions.
- Organize public events, annual hackathons, and cybersecurity challenges tailored to different industries and age groups to showcase career potential
- Provide resources like the Skills Academy Platform (SAP) to help individuals navigate cybersecurity career opportunities.

#### 3.7.1.2 Strategic Goal 2: Encourage Fundamental Computer Science and Informatics Education

Advocate for integrating computer science and informatics into educational curricula from kindergarten through secondary school.

Key Activities:

- Raise awareness about the importance of these subjects in early education.
- Support the Government of the Republic of Slovenia in introducing a compulsory basic skills course, including cybersecurity, to primary and secondary schools by 2025.

## 3.7.2 Medium-term Strategic Goals (3-5 Years)

### 3.7.2.1 Strategic Goal 3: Expand Education and Training Programs

Address the shortage of cybersecurity education by offering new programs with flexible and modular designs to accommodate diverse audiences.

Key Activities:

- Develop specialized training programs at various levels (e.g., entry-level and advanced).
- Integrate soft skills, such as communication, teamwork, problem-solving, and ethical behaviour, into technical training.
- Promote the benefits of these programs to attract a broader audience.

### 3.7.2.2 Strategic Goal 4: Strengthen Industry-Education Collaboration

Align educational offerings with industry needs and emerging trends.

Key Activities:

- Foster partnerships between higher education institutions, vocational training providers, and the cybersecurity sector.
- Facilitate joint projects, guest lectures, internships, and research initiatives.

### 3.7.2.3 Strategic Goal 5: Promote Lifelong Learning

Establish mechanisms for continuous professional development in cybersecurity.

Key Activities:

- Promote upskilling and reskilling opportunities for the workforce in collaboration with experienced companies.
- Document and share best practices in lifelong learning within the industry.
- Position Slovenian CyberHub as a platform to accelerate these efforts across all levels.

## 3.7.3 Long-term Strategic Goals (>5 Years)

### 3.7.3.1 Strategic Goal 6: Drive Innovation, Research, and Knowledge Sharing

Advance cybersecurity innovations and address emerging threats through collaboration among academia, industry, and government.

Key Activities:

- Facilitate R&D projects focused on new cybersecurity challenges.
- Organize innovation challenges to engage stakeholders.
- Create a centralized repository of best practices, tools, and case studies for evidence-based decision-making.
- Foster partnerships for innovative solutions to cyber threats, ensuring a dynamic and resilient cybersecurity ecosystem.

### 3.7.3.2 Strategic Goal 7: Sustain a Resilient Cybersecurity Workforce

Ensure a steady inflow of talent and reduce brain drain.

Key Activities:

- Introduce robust lifelong learning opportunities starting from primary and secondary education.
- Regularly assess and adapt strategies to meet evolving challenges and maintain the competitiveness of Slovenia's cybersecurity education ecosystem.

## 3.8 Conclusions

In conclusion, Slovenia's strategic approach to cybersecurity involves collaboration among government, industry, academia, and specialized organizations. By aligning with EU directives and initiatives through Slovenian CyberHub, the country is addressing its skills gap through partnerships, expanded educational offerings, and lifelong learning programs.

Short-term efforts and goals focus on boosting enrolment and flexible training, while long-term strategies aim to sustain a skilled workforce and reduce brain drain. These measures position Slovenia to enhance cybersecurity resilience and competitiveness in the evolving digital landscape.

Through strategic goals, Slovenian CyberHub will strive to create a dynamic and future-ready cybersecurity education framework, bridging current skills gaps and fostering industry-academia collaboration to drive innovation and workforce development to decrease Slovenia's vulnerability to cyber threats.

## 4 Action Plan

Cybersecurity education and training are essential for building a skilled workforce capable of addressing the ever-evolving cyber threats. The action plan outlines the initiatives needed to achieve strategic goals that support the growth of the cybersecurity sector and its broader impact. This plan will serve as the foundation for a detailed activity plan to be developed in T3.1 MS3 Action plan.

The proposed actions are categorized into:

- **Short-term initiatives:** Promoting enrolment in cybersecurity programs and integrating soft skills into primary and secondary school curricula.
- **Medium-term initiatives:** Expanding educational offerings by educational organisations and strengthening collaboration with industry partners.
- **Long-term initiatives:** Fostering lifelong learning and ensuring program sustainability through regular evaluation.

Additionally, an active community of stakeholders is needed to continuously update and align cybersecurity skills needs with industry demands.

### 4.1 Initiative 1: Raise awareness for Cybersecurity profession/professional career opportunities

**Objective:**

- **Promotion of Cybersecurity Careers** with a goal: Raise awareness about the importance of cybersecurity and growing opportunities for future career path. Key activities will include:
  - Launching campaigns to promote cybersecurity professions among children, students, job seekers, and professionals.
  - Organizing public events, hackathons, and cybersecurity challenges to showcase the field's potential. These kinds of activities will be focused on different target groups like different industries and age groups of future cybersecurity experts.
  - Using resources to help individuals navigate career opportunities in cybersecurity (e.g. (d)Academy Skills Platform).
- **Encouragement of fundamental computer science and informatics:**
  - Raise awareness about the importance of including computer science and informatics content into the curricula of kindergartens, primary and secondary schools.
  - Support and follow up on a declaration calling on the Government of the Republic of Slovenia to introduce a compulsory basic skills course, including cybersecurity, to ensure the successful implementation of these initiatives.

Moreover, the Slovenian CyberHub can actively promote diversity in the cybersecurity field by engaging in joint activities with organisations like Women4Cyber.

### 4.2 Initiative 2: Expand education and training programs/offerings

**Objective:** It is vital to expand cybersecurity education and training programs and offerings, as both are currently very limited. It is essential that these programs also include soft skills, such as communication, teamwork and problem-solving.

To be appealing, more accessible and to invite broader audience it would be best to offer flexible or modular designed trainings (e.g. for specialized cybersecurity skills), if possible, the learning offerings could be organized on different levels (e.g. provide entry-level learning opportunities) as well. It is also vital to raise awareness on the educational and training programs, and benefits of the knowledge such programs bring.

### 4.3 Initiative 3: Promote lifelong learning

**Objective:** One of the most important activities for the Slovenian CyberHub should be the promotion of the lifelong learning in the industry to provide an adequate solution and responses on the prevention of future cyberattacks and quick response if these attacks do happen.

The industry is experienced in providing the upskilling opportunities for its workforce on the cybersecurity topics therefore it is highly recommended these best practices get documented and promoted in the Slovenian CyberHub. Therefore, the Slovenian CyberHub can serve as a platform to accelerate upskilling and reskilling efforts at different levels and increase the promotion of the companies which are experienced in this field.

### 4.4 Initiative 4: Innovation, Research & Development and Knowledge sharing

**Objective:** The action plan for Research and Development focuses on advancing cybersecurity innovations and addressing emerging threats through collaborative projects, bringing together academia, industry, and government. To achieve this, the Slovenian CyberHub will establish itself as a collaborative centre of innovation and knowledge-sharing platform, performing various activities:

- **Facilitating research and development projects** focused on emerging cybersecurity challenges, including the creation of a dedicated platform for joint R&D initiatives.
- **Organizing annual hackathons and innovation challenges** to foster new solutions and stimulate engagement from a wide range of stakeholders.
- **Creating a centralized repository of resources**, including best practices, tools and case studies, to support evidence-based decision-making and continuous learning.
- **Encouraging collaboration on innovative solutions to cyber threats** through partnerships and community-driven initiatives, ensuring a dynamic ecosystem that continually advances the cybersecurity landscape.

### 4.5 Conclusions

The outlined action plan serves as a comprehensive roadmap to enhance cybersecurity education, training and innovation in a rapidly evolving digital landscape. By focusing on short-, medium- and long-term initiatives, it strategically promotes awareness, expands educational offerings, fosters lifelong learning and drives research and development in the field of cybersecurity. The Slovenian CyberHub will play a role in bridging the gap between industry demands and skill development, ensuring the current and future workforce is equipped to successfully combat emerging cyber threats. Collaborative efforts with stakeholders, including educational institutions, industry leaders, and organisations will further amplify diversity, accessibility and inclusivity within the sector.

## 5 Evaluation and Monitoring

Effective evaluation and monitoring are essential to ensure the success and sustainability of the Slovenian Cybersecurity Skills Strategy. These processes will enable stakeholders to track progress, identify areas for improvement, and ensure the strategy's goals and activities remain aligned with national and European cybersecurity objectives. This chapter outlines the approach to metrics and monitoring, as well as strategies for continuous improvement.

### 5.1 Metrics and Monitoring

Once the Slovenian Cybersecurity skills strategy is implemented, specific Key Performance Indicators (KPIs) and reporting mechanisms will be defined for each strategic goal by the Slovenian CyberHub to ensure transparency and accountability. These KPIs will serve as measurable benchmarks to evaluate the strategy's effectiveness and impact across its various initiatives and activities. The implementation of cybersecurity skills initiatives in Slovenian CyberHub will be monitored by a dedicated team from the Slovenian CyberHub, which will regularly monitor progress to ensure initiatives remain on track, swiftly identifying any deviations requiring corrective action. In addition, a periodic review process will be established to regularly assess and refine the governance structure, ensuring its effectiveness, relevance, and ability to drive continuous improvement.

To maintain continuous improvement, the CyberHub will:

- **Regularly evaluate progress through KPIs** such as the number of trained professionals, certifications issued, and partnerships formed.
- **Adapt its activities and strategies** based on feedback from stakeholders and emerging cybersecurity trends.
- **Align with national and European cybersecurity initiatives** to ensure relevance and maximize impact.
- **Foster a collaborative culture**, encouraging stakeholders to actively contribute to the hub's mission and activities.

The table below presents examples of potential KPIs that could be adopted:

Initiative	KPI	Metric	Frequency
Raise awareness for Cybersecurity profession	Enrolment rates in cybersecurity programs	Number of new enrolments per term, segmented by demographics (e.g., age, gender, educational background).	Collected at the start of each academic year.
	Completion and Certification Rates of Students in Cybersecurity Training	Percentage of students who complete the program compared to those who initially enrolled, with a focus on completion times and certification success rates.	Collected at the end of each program cycle.
	Employment Rates of Graduates in Cybersecurity Roles (6-12 Months Post-Graduation)	Percentage of graduates employed in cybersecurity-related roles within 6-12 months post-graduation, segmented by role type and industry.	Collected annually.
	Stakeholder Satisfaction Scores	Satisfaction scores collected through structured surveys, with a focus on areas such as curriculum relevance, graduate preparedness, and program flexibility.	Collected annually.
Expand education and training programs/offerings	Number & diversity of cybersecurity training programs	Total count of newly developed or expanded cybersecurity courses/modules (including flexible, modular, and soft-skills components).	Collected annually.

	Participation rates	Total number of participants enrolled in training programs, segmented by experience level (entry-level, intermediate, advanced).	Collected annually.
	Program completion & satisfaction	Completion rates and satisfaction scores for expanded/updated programs (surveys post-completion).	Collected at the end of each academic year.
Promote lifelong learning	Upskilling & reskilling rates	% increase in professionals transitioning from general IT roles to cybersecurity roles (reskilling) or advancing skills (upskilling).	Collected annually.
	Awareness campaigns for lifelong learning	Number of awareness campaigns conducted annually to promote continuous learning opportunities and their impact (measured by increased inquiries or enrolments).	Collected annually.
	Diversity & inclusion metrics	% of participants from underrepresented groups (e.g., women, minorities) in lifelong learning initiatives.	Collected annually.
Innovation, research & development, knowledge sharing	R&D project initiation	Number of collaborative R&D projects launched, involving academia, industry, and government partners.	Collected annually.
	Innovation challenges & hackathons	Number of annual hackathons or innovation challenges conducted and participation levels (teams, individuals, solutions proposed).	Collected annually.
	Research output & publications	Number of research papers, white papers, and case studies published or shared through the CyberHub repository.	Collected annually.

*Table 1: Potential KPIs for each initiative.*

## 5.2 Continuous Improvement

To ensure the Slovenian Cybersecurity Hub's action plan remains responsive to changing conditions and aligned with industry standards, a comprehensive approach to managing the response to changing situations will be established. This includes:

- **Regular monitoring and reporting:** Regular evaluations of KPIs and progress toward strategic goals, with adjustments made as necessary. These reports will provide insights into trends and highlight any emerging issues or shifts in demand, allowing for timely adjustments to maintain program alignment.
- **Environmental scanning and trend analysis:** Routine scans will be regularly conducted across the cybersecurity industry, labour market, and educational landscape to identify emerging trends, technologies, and shifts in employer requirements.
- **Stakeholder feedback:** Regular feedback sessions will be held with industry partners, government bodies, students, and educators to gauge their perception of the program's relevance, strengths, and improvement areas. This feedback will be incorporated into ongoing reviews of KPIs and activities, ensuring the program continues to meet the evolving needs of all stakeholders.
- **Agility in response to immediate changes:** Should a significant shift occur—such as a sudden demand for specific cybersecurity skills or updates to industry standards—the program team may initiate an immediate review of related activities. This enables a faster, adaptive response to maintain alignment with external requirements, ensuring the program's ongoing relevance and effectiveness.

## 5.3 Conclusions

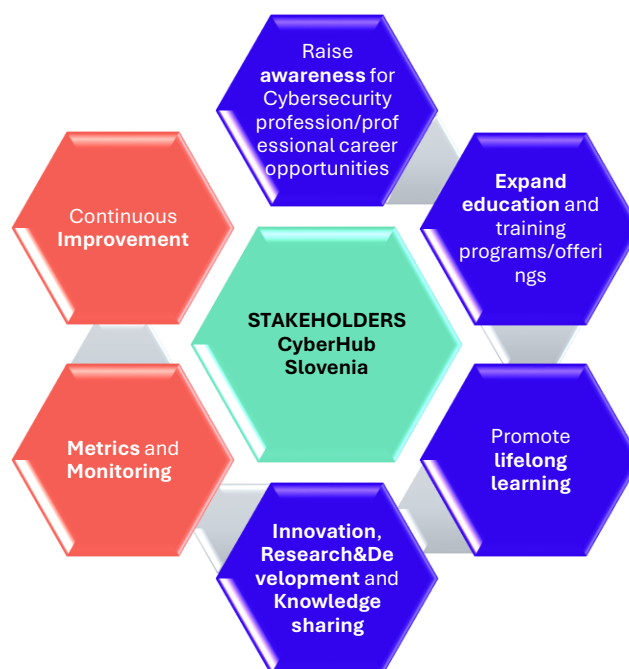
The implementation and ongoing evaluation of cybersecurity skills initiatives in Slovenia, led by the CyberHub Slovenia, represents a strategic effort to address the nation's growing cybersecurity needs. By establishing a system of KPIs, monitoring and reporting processes, these initiatives ensure cybersecurity educational and training programs are responsive, relevant, and aligned with industry demands. The structured approach to continuous improvement provides a dynamic framework that can adapt to evolving requirements. This adaptability not only supports the immediate goals for developing current and future skilled cybersecurity workforce but also contributes to a resilient national cybersecurity infrastructure that can keep pace with technological advancements and emerging threats.

## 6 Conclusions

With this document, CyberHub Slovenia confirms its commitment to building a skilled cybersecurity workforce, which is the cornerstone of national security, EU security and the wider digital economy. Slovenia stands at a critical juncture in its journey to strengthen its cybersecurity landscape. The growing risks posed by cyber threats, the rise of artificial intelligence, and stricter regulatory frameworks such as the NIS2 Directive underscore both the urgency and complexity of the challenges ahead. Despite a robust framework of key actors—government entities, educational institutions, and industry stakeholders—the country continues to face a substantial cybersecurity skills gap, compounded by limited specialized educational programs and an evolving regulatory environment.

In response to these challenges, Slovenia is establishing the **Slovenian CyberHub**, envisioned as a central platform to foster collaboration, drive educational changes and accelerate innovation. The infographic on Figure 2 visually represents the CyberHub stakeholders at the centre of key focus pillars:

1. **Raise Awareness for Cybersecurity Profession/Professional Career Opportunities**
2. **Expand Education and Training Programs/Offerings**
3. **Promote Lifelong Learning**
4. **Innovation, Research & Development, and Knowledge Sharing**
5. **Metrics and Monitoring**
6. **Continuous Improvement**



*Figure 2: CyberHub Slovenia Key Pillars of Skills Development*

Each of these interconnected areas underscores the strategy's multifaceted approach to building a robust cybersecurity ecosystem: from cultivating a steady pipeline of skilled professionals to continuously monitoring and refining programs in alignment with emerging threats and industry demands. Acting on insights from the D2.1 Cybersecurity Skills Needs Analysis report, the CyberHub will drive a multi-phased strategy targeting immediate, medium-term, and long-term

goals, ensuring that Slovenia not only closes its current gaps but also positions itself as a competitive player in the global cybersecurity area.

By raising awareness of cybersecurity careers, expanding training opportunities, and promoting lifelong learning, Slovenia aims to transform its vulnerabilities into opportunities for growth. Meanwhile, the **Slovenian Cybersecurity Skills Strategy** provides a framework of clear metrics and a robust monitoring process, ensuring that progress remains aligned with both national and European objectives.

Ultimately, achieving this vision requires coordinated efforts from all stakeholders. Through proactive engagement across government, academia, and industry, Slovenia can develop and maintain the skilled cybersecurity professionals needed to protect its digital economy.

## 7 References

1. Naslovnica - SI CERT. Online. [Accessed 12 December 2024]. Available from: <https://www.cert.si/>
2. Cybercrime To Cost The World 8 Trillion Annually In 2023. Online. [Accessed 11 December 2024]. Available from: <https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>
3. Institute for Security and Technology 2023 RTF Global Ransomware Incident Map: Attacks Increase by 73%, Big Game Hunting Appears to Surge - Institute for Security and Technology. Online. [Accessed 11 December 2024]. Available from: <https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map/>
4. How Many Cyber Attacks Happen Per Day in 2023? - Security Boulevard. Online. [Accessed 11 December 2024]. Available from: <https://securityboulevard.com/2023/11/how-many-cyber-attacks-happen-per-day-in-2023/>
5. ZAKON O INFORMACIJSKI VARNOSTI (ZINJV). [Accessed 20 January 2025].
6. ZAKON O VARSTVU OSEBNIH PODATKOV (ZVOP-2). [Accessed 20 January 2025].
7. ZAKON O ELEKTRONSKIH KOMUNIKACIJAH (ZEKOM-2). [Accessed 20 January 2025].
8. Cybersecurity Skills Needs Analysis in Slovenia - CyberHubs. Online. [Accessed 11 December 2024]. Available from: <https://cyberhubs.eu/resource/cybersecurity-skills-needs-analysis-in-slovenia/>



**European Network of Cybersecurity Skills Hubs**

[info@cyberhubs.eu](mailto:info@cyberhubs.eu) | [cyberhubs.eu](https://cyberhubs.eu)



**Co-funded by  
the European Union**

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 Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.