CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

D1.1
Training and knowledge transfer needs and opportunities (SWOT) in the selected areas of cybersecurity R&I in South Moravia and Estonia.

Project Name	Cyber-security Excellence Hub in Estonia and South Moravia
Project acronym	CHESS
Grant agreement no.	101087529
Call	HORIZON-WIDERA-2022-ACCESS-04
Type of action	HORIZON-CSA
Project starting date	1 January 2023
Project duration	48 months
Deliverable Number	D1.1
Deliverable name	Training and knowledge transfer needs and opportunities (SWOT) in the selected areas of cybersecurity R&I in South Moravia and Estonia.
Lead Beneficiary	CSH
Type	R — Document, report
Dissemination Level	PU - Public
Work Package No	WP1
Date	02 August 2024
Version	2

Funded by the European Union

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Editor

- Václav Stupka (CSH)
- Hendrik Pillmann (RIA)

Contributors

- Raimundas Matulevičius (UTARTU)
- Lukáš Malina (BUT)
- Václav Matyáš (MUNI)
- Liina Kamm (CYBER)
- Antonín Kučera (MUNI)
- Pawel Sobocinski (TalTech)
- Mubashar Iqbal (UTARTU)
- Petr Švenda (MUNI)
- Jan Willemson (CYBER)
- Jan Hajný (BUT)
- Pavel Čeleda (MUNI)
- Martin Ukrop (Red Hat)
- Alo Lilles (Guartime)

Reviewers

- Zuzana Vémolová (MUNI)
- Václav Matyáš (MUNI)

CHESS Consortium

Participant organisation name	Short name	Country
Masaryk University	MUNI	Czechia
University of Tartu	UTARTU	Estonia
Brno University of Technology	BUT	Czechia
Tallinn University of Technology	TalTech	Estonia
Cybernetica AS	CYBER	Estonia
Red Hat	RedHat	Czechia
Guardtime	Guardtime	Estonia
Estonian Information System Authority	RIA	Estonia
CyberSecurity Hub	CSH	Czechia
National Cyber and Information Security Agency (associated)	NCISA	Czechia
South Moravian Innovation Centre (associated)	JIC	Czechia
Estonian Information Security Association (associated)	EISA	Estonia

Abbreviations

CA – Challenge Area
CHESS – Cyber-security Excellence Hub in Estonia and South Moravia
ICT – information and communication technology
KPI – key performance indicator
NGO – non-governmental organisation
OA – open access
R&I – research and innovation
TA – target audience
WP – work package
R&I – research and innovation
IoST – Internet of Secure Things
NCSC-EE – National Cyber Security Center
CERT-EE – Estonian Computer Emergency Response Team
CSIRT – Computer Security Incident Response Team
ITS – Intelligent Transportation Systems
AI/ML – Artificial intelligence/machine learning

Executive Summary

The CHESS project, focusing on cybersecurity research and innovation (R&I) in South Moravia and Estonia, has undertaken a comprehensive analysis to identify the training and knowledge transfer needs and opportunities in these regions. This deliverable encompasses a detailed SWOT analysis, capturing the strengths, weaknesses, opportunities, and threats associated with the cybersecurity ecosystems of both regions. The analysis has been integral in outlining the current state of cybersecurity and in setting the strategic direction for future collaborative efforts.

Key Findings

Conducted SWOT analyses identify these common key findings that are apparent in individual challenge areas:

- **Strengths** in both regions include robust academic foundations, vibrant technological ecosystems, and strong collaborations between research institutions and industry.
- **Weaknesses** involve challenges such as fragmented regulatory environments, a need for greater investment in advanced technological infrastructures, and a lack of comprehensive strategies for SME engagement in cybersecurity initiatives.
- **Opportunities** presented by the expanding digital economy and the rising importance of cybersecurity on the global stage offer both regions the potential to enhance their international standing and technological advancements.
- **Threats** include the increasing sophistication of cyber-attacks, rapid technological changes outpacing current security measures, and potential funding instabilities.

Strategic Recommendations

The comprehensive analysis conducted in this document led to the identification of the set of strategic recommendations that are designed to address the core challenges and harness the opportunities within the cybersecurity landscapes of South Moravia and Estonia. These recommendations aim to fortify the regions' cybersecurity infrastructures and capabilities. The recommendations include:

- **Enhance Intersectoral Collaboration**: Establish stronger networks across academia, industry, and government to foster innovation and effective translation of research into practice.
- **Bolster Education and Training**: Expand cybersecurity training programs to develop a skilled workforce that is equipped to handle emerging cyber threats.
- **Strengthen International Partnerships**: Engage more actively in international cybersecurity initiatives to benefit from and contribute to global security standards and practices.

By implementing these strategic actions, both regions can effectively improve their resilience to cyber threats and elevate their status as innovators and leaders in the global cybersecurity arena.

Action Plan

The action plan developed from this analysis advocates for targeted initiatives aimed at strengthening the cybersecurity infrastructure, enhancing collaborative research and innovation activities, and promoting effective knowledge transfer among stakeholders. This includes:

- Developing a cross-regional R&I strategy to address specific cybersecurity challenges.
- Implementing structured knowledge-sharing and training initiatives.
- Enhancing funding mechanisms to support sustainable cybersecurity advancements.

Conclusion

This deliverable lays a foundational analysis for the CHESS project, providing a clear direction for future initiatives aimed at enhancing the cybersecurity capabilities of South Moravia and Estonia. By addressing the identified challenges and leveraging the opportunities for growth and improvement, these regions can enhance their resilience against cyber threats and position themselves as leaders in the field of cybersecurity research and innovation. This executive summary encapsulates our findings and recommendations, setting the stage for impactful, long-term advancements in regional and global cybersecurity landscapes.

Table of Contents

List of Tables

1 Introduction

In the current era, where digital threats are evolving with unprecedented speed and complexity, the imperative for robust cybersecurity research and innovation (R&I) has never been more critical. The collaborative project between South Moravia and Estonia represents a strategic initiative aimed at harnessing the collective strengths and capabilities of both regions to advance the state of cybersecurity R&I. This deliverable, D1.1, focuses on identifying the training and knowledge transfer needs and opportunities within selected areas of cybersecurity R&I, leveraging the standard SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis framework. The document offers an overview of cybersecurity ecosystems in both regions, identifies key stakeholders and the existing cross-regional and cross-sectoral links in six Challenge Areas. Based on this SWOT analysis and the needs identified, the consortium will later prepare a cross-regional cybersecurity R&I strategy and an action plan for each Challenge Area. This analysis will help design the right training, plan inter-sectoral and/or inter-regional knowledge exchange by means of specialized events and fellowships, design and target outreach activities more effectively and plan future research activities.

Context

South Moravia and Estonia, both recognized for their vibrant technological ecosystems and innovative capacities, offer unique yet complementary assets in the realm of cybersecurity. South Moravia, with its strong academic foundations and burgeoning tech industry, and Estonia, renowned for its digital government and cybersecurity advancements, are poised to collaborate effectively in addressing the emerging challenges in cybersecurity. This deliverable seeks to map out the capacities, expertise, value chains, common interests and needs in both regions, laying the groundwork for a strategic partnership in cybersecurity R&I.

Objectives

The primary objective of this deliverable is to provide a comprehensive analysis of the training and knowledge transfer needs and opportunities in the selected areas of cybersecurity R&I in South Moravia and Estonia. By doing so, it aims to:

- Identify and evaluate the existing capacities and expertise in both regions.
- Analyse the value chains within the selected areas of cybersecurity R&I.
- Highlight the common interests and needs that could foster collaboration and innovation.
- Offer a SWOT analysis to inform strategic decision-making and policy development.

Scope

This analysis covers selected areas of cybersecurity R&I deemed critical for the advancement of both regions' cybersecurity capabilities. These areas were chosen based on their relevance to the current and future security landscape, the potential for impact, and the existing strengths and opportunities within South Moravia and Estonia. The deliverable will not encompass all aspects of cybersecurity but will focus on those areas identified through a collaborative and consultative process involving key stakeholders from both regions.

This deliverable therefore aims to provide a clear and structured analysis that will guide the strategic direction of cybersecurity R&I collaboration between South Moravia and Estonia. Through this endeavour, both regions aspire to not only enhance their own cybersecurity landscapes but also contribute to the global effort in securing digital infrastructures and information.

2 Methodology

To construct a comprehensive methodology for this deliverable, a multi-dimensional approach was designed and implemented. This approach integrates data from structured questionnaires and extensive desk research, ensuring a robust foundation for the analysis and findings presented. The following sections detail each component of the methodology, emphasising the processes of data collection, analysis, and synthesis.

Structured Questionnaire

The initial phase of data collection involved the design and distribution of a structured questionnaire, targeting a broad spectrum of stakeholders within the cybersecurity research and innovation (R&I) community in South Moravia and Estonia. The questionnaire was crafted to elicit both quantitative and qualitative responses across various dimensions critical to understanding the cybersecurity ecosystem, including regional academic and industry expertise, collaboration within and across regions, and the broader European and global context of cybersecurity R&I.

The distribution strategy aimed to ensure a diverse and representative sample of respondents, encompassing academic institutions, research teams, companies, governmental bodies, and other entities actively engaged in cybersecurity. This diversity was crucial for capturing a holistic view of the cybersecurity landscape, encompassing different perspectives and experiences. The analysis of questionnaire responses employed statistical methods for quantitative data and content analysis for qualitative insights, facilitating a comprehensive understanding of the current state, challenges, and opportunities within the cybersecurity R&I domain.

Desk Research

Desk research constituted a significant component of the methodology, involving a thorough review of existing literature, public sources, and information available to the project partners. This review spanned academic publications, industry reports, policy documents, and online databases, focusing on sources that provided insights into the cybersecurity R&I landscape, trends, challenges, and opportunities. The desk research was designed to complement the primary data collected through questionnaires and interviews, providing a broader context and supporting evidence for the analysis.

Relevant information extracted from the desk research was synthesised with the primary data, enriching the analysis and ensuring a comprehensive understanding of the cybersecurity domain. This synthesis involved identifying corroborating evidence, contrasting viewpoints, and additional data points that provided depth and context to the findings.

Integrated Data Analysis and Synthesis

The integration of data from the questionnaires, interviews, and desk research was a critical step in the methodology. This process involved triangulating data from different sources to validate findings, identify patterns and trends, and ensure a robust analysis. The thematic synthesis combined insights from qualitative analyses with quantitative data trends, facilitating a nuanced understanding of the cybersecurity R&I ecosystem. The development of the SWOT analysis, a foundational element of the deliverable, was informed by the integrated data analysis. This analysis identified the strengths, weaknesses, opportunities, and threats related to cybersecurity R&I in South Moravia and Estonia, highlighting areas for potential training and knowledge transfer.

Limitations

The methodology also acknowledges potential limitations, such as response bias and the representativeness of the sample. Strategies to mitigate these limitations included the use of multiple data sources and a critical evaluation of findings in the context of existing literature and known facts about the cybersecurity landscape.

The methodology employed for Deliverable D1.1 represents a comprehensive and rigorous approach to understanding the training and knowledge transfer needs and opportunities within the cybersecurity R&I ecosystem in South Moravia and Estonia. By integrating data from structured questionnaires and extensive desk research, the methodology ensures that the findings and recommendations are grounded in a rich dataset, offering actionable insights for advancing cybersecurity R&I in the regions.

3 Analysis

The cybersecurity landscape is rapidly evolving, driven by technological advancements and the increasing sophistication of cyber threats. In this context, the cybersecurity research and innovation (R&I) ecosystems in South Moravia and Estonia play a pivotal role in developing resilient and advanced security solutions. This analysis aims to dissect the current state and market potential of the cybersecurity sector in these regions, offering a detailed examination of the ecosystem as a whole and delving into specific challenge areas critical to advancing the field.

The first part of the analysis provides an overarching view of the cybersecurity R&I ecosystem, exploring the regulatory environment, funding sources, support structures, and mechanisms fostering cross-sectoral cooperation. It aims to map out the key stakeholders, including research institutions, public institutions, companies, and other actors, whose collaborative efforts are essential for the sector's growth and innovation.

The second part focuses on specific challenge areas that are at the forefront of cybersecurity concerns: Internet of Secure Things (IoST), Security Certification, Verification of Trustworthy Software, Security Preservation in Blockchain, Post-Quantum Cryptography, and Human-Centric Aspects of Cyber-Security. For each area, this analysis will outline the current situation, stakeholder dynamics, examples of good practice, and a SWOT analysis to identify areas of strength, potential improvements, and future opportunities for advancement.

This comprehensive analysis aims to provide actionable insights and recommendations to support the continued growth and effectiveness of the cybersecurity R&I ecosystem in South Moravia, Estonia, and beyond, ensuring its relevance and impact within the broader European context.

3.1 Overview of the Cybersecurity Ecosystems

The cybersecurity ecosystem, encompassing a complex network of stakeholders, technologies, regulations, and market dynamics, is foundational to the digital security and resilience of nations. In the context of South Moravia and Estonia, two regions with distinct yet complementary strengths in research and innovation (R&I), understanding the overarching cybersecurity landscape is crucial. This part of the analysis aims to provide a comprehensive overview of the cybersecurity ecosystem within these regions, focusing on:

- **Regulatory Environment** The regulatory framework sets the legal and operational boundaries for cybersecurity activities, influencing how research, development, and implementation of cybersecurity solutions are conducted. This section will explore the specific regulations, policies, and standards that shape the cybersecurity R&I landscape in South Moravia and Estonia, highlighting similarities, differences, and the impact of European Union directives and regulations.

- **Funding Sources** Funding is the lifeblood of innovation, particularly in a field as dynamic and resource-intensive as cybersecurity. This analysis will detail the various public and private funding mechanisms available to support cybersecurity R&I in both regions, including government grants, European funding programs, venture capital, and other financial instruments. The aim is to understand how these funding sources are accessed and utilized by the cybersecurity sector and how they drive the development of new technologies and solutions.

- **R&I Support Structures & Cross-Sectoral Cooperation** Support structures, such as technology parks, incubators, accelerators, and research consortia, play a pivotal role in nurturing innovation and facilitating the translation of research into market-ready solutions. This section will evaluate the existing support structures dedicated to cybersecurity R&I in South Moravia and Estonia, assessing their effectiveness and the extent to which they are leveraged by the sector. The interdisciplinary nature of cybersecurity necessitates collaboration across various sectors, including information technology, telecommunications, finance, and defence; this analysis will therefore also examine the instruments and best practices that promote cross-sectoral cooperation in cybersecurity R&I, identifying successful models of collaboration that could be replicated or scaled.

- **Key Stakeholders** Identifying and understanding the roles of key stakeholders within the cybersecurity ecosystem is essential for fostering cooperation and driving innovation. This section will provide an overview of the major stakeholders in South Moravia and Estonia, including research institutions, public institutions, companies, and other entities. The focus will be on how these stakeholders contribute to the cybersecurity landscape, their areas of expertise, and how they collaborate to address cybersecurity challenges.

Through this detailed examination of the cybersecurity ecosystem in South Moravia and Estonia, this analysis seeks to lay the groundwork for identifying opportunities for growth, enhancement of R&I capabilities, and strengthening of the regions' positions within the broader European cybersecurity landscape.

3.1.1 Introduction to the Ecosystems

The cybersecurity landscapes in South Moravia and Estonia serve as exemplary models of innovation and dynamism, each characterised by unique attributes and contributions to the field. This analysis seeks to delve into these ecosystems, highlighting the regulatory frameworks, funding mechanisms for cybersecurity research and innovation (R&I), strategies for fostering cross-sectoral collaboration and identifying the principal actors within each region. The aim is to understand the factors that underpin the growth of technological startups, the synergies between academic institutions and the industry, and the overall advancement of the cybersecurity sector within these locales.

Cybersecurity Innovation in South Moravia

Dubbed the "Czech Silicon Valley," South Moravia stands out for its dense concentration of software development firms, SMEs, and startups, particularly those engaged in creating cutting-edge ICT solutions. The region's notable impact on the Czech Republic's Digital Economy and Society Index (DESI) rankings highlights its leadership in e-commerce and digital technology adoption across Europe. However, it faces challenges in elevating its e-government services to match its digital achievements elsewhere.

The success of South Moravia is anchored in a robust public research infrastructure, the establishment of major development centres by global cybersecurity leaders, and a culture of collaboration between the public sector, corporate sector and academia. This tripartite synergy fosters an environment ripe for innovation and advancement in the field of cybersecurity.

Central to the region's research infrastructure are its leading universities, which are pivotal in driving forward the cybersecurity agenda. Masaryk University, which is the second largest university in Czechia, deals with cybersecurity using a multidisciplinary approach. Its research teams focus not only on technical issues at Faculty of Informatics and Institute of Computer Science (cryptography, detection and mitigation of cybersecurity incidents, development of cyber ranges and platforms for cybersecurity training, secure software development, protection of critical infrastructures, etc.) but also societal issues at Faculty of Social Science (cybersecurity policy governance) and legal issues at Institute of Law and Technology (data protection law, cybersecurity law, ISP compliance, fundamental rights and compliance, jurisdiction and internet governance, etc.). The Brno University of Technology (BUT) complements this with its specialized programs and research projects aimed at pushing the boundaries of cybersecurity knowledge and application. The key teams focusing on Cybersecurity are based at the Faculty of Electrical Engineering (FEKT BUT) and the Faculty of Information Technology (FIT BUT). The focus is mainly on basic-oriented and applied research in various technological areas (cryptography, post-quantum, critical infrastructures cybersecurity, digital forensics, AI cybersecurity, etc.).

The corporate sector in the South Moravian Region is marked by a vibrant mix of global IT companies and innovative startups. Notably, companies like RedHat, Oracle, AT&T, SolarWinds or Honeywell have established significant development centres in the region, contributing to its reputation as a hub for IT innovation. These companies not only stimulate local economic growth but also offer fertile ground for collaboration with academic institutions.

Public institutions are integral to the cybersecurity ecosystem in the region. All key government agencies that deal with cybersecurity are located in Brno. National Cyber and Information Security Agency is the key cybersecurity public institution involved both in regulation, oversight and awareness raising in the area, Military Intelligence operates National Centre for Cyber Operations which is responsible for cyber defence, Prosecutor General’s office and key higher courts (Constitutional court, Supreme court and Supreme administrative courts) offer cooperation on issuer related to fight against cybercrime and Data Protection Office deals with oversight over protection of personal data.

Cooperation and coordination of all these key stakeholders underscores a national commitment to advancing cybersecurity strategies and solutions. Nonetheless, there's room for improvement, especially in SMEs' digital intensity and the provision of some e-government services.

Estonia's Digital Governance and Cybersecurity Excellence

Estonia is renowned for its strong association with government initiatives and its leading position in Europe for e-government indicators. The country's advanced digital public services, strategic development of human capital in the ICT field, and forward-thinking approach to public e-services and cybersecurity risks are globally recognized.

While South Moravia is praised for fostering a conducive environment for ICT innovation and growth, Estonia stands out for its outstanding digital governance and framework for e-services. Estonia is distinguished from South Moravia by its dynamic ecosystem of technology start-ups, research institutions and IT companies. The triumph of Estonia's tech ecosystem stems from a strong public research infrastructure, complemented by significant development hubs established by worldwide cybersecurity leaders and a collaborative approach among public, private, and academic entities. This synergy encourages an environment that promotes innovation and advancement in cybersecurity.

At the core of Estonia’s research infrastructure lies its leading universities, which are pivotal in shaping the cybersecurity landscape. **The University of Tartu (UTARTU)**, recognised as Estonia's premier academic institution, employs a multidisciplinary approach to cybersecurity. Its research teams address technical challenges while also analysing societal and legal aspects. Additionally, **Tallinn University of Technology (TalTech)** complements these efforts with specialised programs and research projects aimed at advancing knowledge and applications in cybersecurity. Key research teams specialising in cybersecurity operate within these institutions, contributing to various technological domains such as cryptography, post-quantum technologies, cybersecurity for critical infrastructures, digital forensics, and AI cybersecurity.

Estonia's corporate landscape showcases a vibrant combination of global IT giants and pioneering startups. Estonia has served as an environment for innovative projects and original approaches (e.g., solutions created by Skype, Wise and Pipedrive, etc). It is important to highlight that the environment has also fostered the emergence of cybersecurity companies (including research-intensive companies) in the market (representatives of the cybersecurity field, such as Cybernetica, Cybers, SK-ID Solutions, CybExer Technologies, GuardTime, etc).
Public institutions play a vital role in Estonia’s cybersecurity ecosystem, with key government agencies specialising in cybersecurity.

At the national level in Estonia, the responsibility for overall cybersecurity strategy and policy development lies with the **Ministry of Economic Affairs and Communications**. Under the jurisdiction of the Ministry of Economic Affairs and Communications is the Estonian central cyber security institution - the **National Information System Agency (Estonian Information System Authority, also known as RIA).** One pillar of RIA ensures the interoperability of the state’s central information systems, while the other, the **National Cyber Security Center (NCSC-EE)**, ensures the security of those systems and handles security incidents in Estonian computer networks. Among the responsibilities of NCSC-EE are national-level cyber threat assessments, cybersecurity awareness activities, development and implementation of the national information security standard, ensuring the cybersecurity of critical sector operators, and national cyber crisis management readiness. Estonian-only governmental **CERT-EE** is part of the NCSC-EE and a member of the CSIRTs Network.

Cyber diplomacy is in the portfolio of the **Ministry of Foreign Affairs**, and cyber activities related to national defence is under the jurisdiction of the **Ministry of Defence**. The **Cybercrime Unit C3EE**, which is part of the **Police and Border Guard Board (PPA)** under the **Ministry of the Interior**, deals with the prevention and pre-trial investigation of cybercrime. Additionally, Estonia is a party to the Budapest Convention in 2004 and signed the Second Additional Protocol in 2022.

The activities of all these institutions are coordinated by an inter-agency body, the **Cyber Security Council**, which is led and managed by the Ministry of Economic Affairs and Communications. The Cyber Security Council meets regularly, ensures strategic-level inter-agency cooperation, and oversees the implementation of Cyber Security strategy objectives. Headed by the Secretary General of the Ministry of Economic Affairs and Communications, this Council is responsible to the Security Committee of the Estonian Government. In addition, various cyber coordination formats have been launched, perhaps the most important of which is the **Cyber Policy Board**, which consists of representatives of state institutions, the private sector and the academy.

Estonia has an official position on the application of international law, including human rights, in the context of cyber operations and stands for the applicability of existing international law in cyberspace. Both at times of peace and war, states must act responsibly in cyberspace.

Estonian armed forces have designated Cyber Command since 2018. Its primary mission is to carry out operations in cyberspace in order to provide command support for the **Ministry of Defence's** area of responsibility. In addition to the Ministry of Defence, national cyber defence is supported by **the Estonian Defence League's Cyber Defence Unit** that includes cyber security professionals from both public and private entities.
The collaboration and coordination among these stakeholders underscore Estonia's dedication to advancing cybersecurity strategies and solutions. However, there is still room for improvement, particularly in enhancing the digital capabilities of SMEs and further developing e-government services.

Comparative Insights and Regional Synergies

The examination of South Moravia's and Estonia's cybersecurity ecosystems reveals the pivotal role of governmental support, academic-industry partnerships, and targeted legislative measures in propelling the cybersecurity domain. While South Moravia is celebrated for creating a fertile ground for ICT innovation and development, Estonia is renowned for its exemplary digital governance and e-services framework. Each region's approach to nurturing cybersecurity R&I, from their funding landscapes to regulatory environments, showcases tailored strategies to capitalize on inherent strengths and mitigate specific challenges.

This analysis will further scrutinise how these ecosystems leverage their unique capabilities to encourage cross-sectoral cooperation, assess the impact of their R&I support frameworks, and explore the involvement of key stakeholders in advancing the cybersecurity field. Through this comparative lens, we aim to unearth best practices and avenues for cross-learning and collaboration between South Moravia and Estonia, enriching the broader European narrative on cybersecurity innovation and resilience.

3.1.2 Regulatory Environment

While both are aligned with European Union directives and regulations, the regulatory environments for cybersecurity in the Czech Republic and Estonia reflect distinct national priorities and strategies shaped by their unique geopolitical and digital landscapes. As EU member states, both countries adhere to overarching EU cybersecurity frameworks, such as the Network and Information Security (NIS and NIS2) Directive, the Cybersecurity Act and the General Data Protection Regulation (GDPR), yet their implementation and national strategies reveal differing approaches to cybersecurity governance.

Czech Republic: A Comprehensive Approach to Cybersecurity Regulation

The Czech Republic has established a robust regulatory framework for cybersecurity, underpinned by Act No. 181/2014 Coll., on Cyber Security, and subsequent amendments. This legislation sets out the responsibilities of state bodies, critical infrastructure operators, and important information systems operators in ensuring cybersecurity. The Czech approach emphasizes the protection of critical infrastructure and the establishment of the National Cyber and Information Security Agency (NÚKIB) as the central administrative body for cybersecurity. NÚKIB's role includes issuing binding instructions to rectify identified vulnerabilities, a testament to the Czech Republic's proactive stance on cybersecurity threats.

Czechia is currently set to update the Act on Cybersecurity significantly. This legislative revision aims to bolster the nation's defences against cyber threats by introducing comprehensive regulations required by EU NIS2 regulation and to include new mechanisms for cybersecurity certification and supply chain supervision. By establishing stringent cybersecurity certification frameworks and ensuring rigorous supervision of supply chains, the new act seeks to mitigate sophisticated cyber threats and foster a unified approach to digital security within the EU. The revision of the Czech Act on Cybersecurity marks a key step in strengthening the nation's cybersecurity infrastructure. It not only elevates the security of key services but also addresses the complex challenges posed by the globalization of digital services and their supply chains. The revision also expands the reach of current legislation because the number of regulated entities will rise to about 6000; this will lead to a higher level of infrastructure security but also a higher cost of cybersecurity compliance.

Moreover, the Czech Republic's cybersecurity strategy is integrated into broader national security and defence policies, reflecting its prioritisation of cybersecurity as a national security issue. This integration is facilitated by the country's strategic position in Central Europe and its active participation in international cybersecurity initiatives, including those of NATO and the EU. The strategy is also amended by an action plan that aims to address key identified issues in policy, capacities and cooperation among key stakeholders.

While the Czech Republic's Cybersecurity Strategy and Act lays the foundational framework for securing key infrastructures, it is complemented by a tapestry of sectoral and specific legislation that addresses security requirements across various domains. This includes the Act on Information Systems of the Public Sector, the Act on Electronic Communication, and data protection legislation, alongside regulations specific to the financial, energy, and health sectors, among others. Each piece of legislation tailors cybersecurity measures to the unique needs and vulnerabilities of these sectors, ensuring a comprehensive and cohesive approach to safeguarding the nation's digital landscape. This multi-layered legal structure reflects the understanding that cybersecurity is not a one-size-fits-all issue but requires nuanced and sector-specific strategies to effectively protect against evolving cyber threats.

Integral to the legislative framework governing cybersecurity in the Czech Republic are laws designed to combat cybercrime, primarily embodied in the Criminal Code and the Criminal Procedure Code. These legal instruments provide the judicial system with the necessary authority and procedures to identify, prosecute, and penalise cybercriminal activities, ranging from data breaches and unauthorised access to more sophisticated cyber fraud and attacks. By clearly defining cybercrime offences and establishing the legal groundwork for investigation and prosecution, these codes play a crucial role in the nation's broader cybersecurity strategy, ensuring that perpetrators of cybercrime face justice and reinforcing the legal deterrents against such activities.

Completing the comprehensive cybersecurity legislation in the Czech Republic, the Act on Military Intelligence plays a pivotal role by equipping military intelligence with the necessary powers and competencies to ensure robust cyber defence. This act authorises the building of essential capacities and oversight over Czech information infrastructures, thereby fortifying the nation's defence against cyber threats. This act underscores the importance of a multi-faceted approach to cybersecurity, integrating national defence mechanisms with civilian cybersecurity efforts to create a resilient and secure digital environment.

The Czech legal environment for cybersecurity represents a comprehensive and multi-layered framework designed to address the multifaceted challenges of securing digital spaces and combating cybercrime. By integrating the foundational Cybersecurity Act with sector-specific legislation, criminal codes aimed at fighting cybercrime, and the Act on Military Intelligence for national defence, the Czech Republic has established a robust legal infrastructure that spans across civilian and military domains. This cohesive approach not only ensures the protection of critical information infrastructures and the public sector but also empowers law enforcement and military intelligence to effectively counter cyber threats. As the digital landscape continues to evolve, this legal framework positions the Czech Republic to adapt and respond to emerging cybersecurity challenges, safeguarding the nation's digital future while aligning with broader European Union legislation and standards.

Estonia: Pioneering Digital Governance and Cybersecurity

Estonia's regulatory environment for cybersecurity is arguably one of the most advanced globally, largely due to its pioneering status in e-governance and digital public services. RIA plays a pivotal role in overseeing the country's cybersecurity, similar to the NÚKIB in the Czech Republic. Estonia's approach is encapsulated in its Cybersecurity Strategy, with recent updates reflecting the evolving nature of cyber threats and the digital economy.

Estonia's regulatory framework is designed to protect its extensive digital infrastructure, which supports a wide array of e-services, from e-voting to digital health records. The country's legislation emphasises not only the security of digital services but also the resilience of the digital society against cyber threats. This focus is a direct response to Estonia's experiences with cyber-attacks, most notably the 2007 attacks that targeted its national infrastructure, leading to a comprehensive overhaul of its cybersecurity policies and systems. In addition to the regulatory framework, Estonia's commitment to cybersecurity is further bolstered by its investment in education and awareness programs. The country prioritises cybersecurity education from an early age, integrating it into school curriculums and offering specialised training programs for professionals. This proactive approach ensures that the workforce is equipped with the necessary skills and knowledge to address emerging cyber threats effectively.

Furthermore, Estonia actively participates in international cybersecurity cooperation initiatives, recognising the interconnected nature of cyber threats and the importance of collaboration on a global scale. By sharing best practices, information, and resources with other nations, Estonia contributes to the collective effort to enhance cybersecurity resilience worldwide.

Since 2018, the central legal document in the field of cyber security in Estonia is the Cyber Security Act, which, among other things, adopted Directive (EU) 2016/1148 of the European Parliament and of the Council (NIS1). Accordingly, in Estonia, operators of critical (information) infrastructure are required to assess and manage cyber risks, implement cybersecurity measures, and report cybersecurity incidents. In 2022, Directive (EU) 2022/2555 of the European Parliament and of the Council, or NIS2, was adopted at the EU level, which significantly complements the provisions of the previous directive and is now being transposed into Estonian law. In addition, specific cyber-security requirements for the financial sector have been established. The new EU regulatory initiatives for critical service providers and manufacturers in the field of cyber security, for example, the Cyber Resilience Act, Cyber Solidarity Act or Cyber Security Act, will be adopted to Estonian legislation.

Initiated shortly after the wave of cyberattacks in 2007, Estonia's first cyber security strategy was developed for 2008-2013, which at that time placed the country among the very few that had such a national development plan. In 2013, the second strategy was developed for the period 2014-2017, and in 2018, the third version of the strategy was approved by the government for 2019-2022. The development of the fourth-generation strategy for 2024-2027 is underway. The strategic planning of cybersecurity throughout the strategic lifecycles has had a significant positive impact on the Estonian cybersecurity situation as well as on the development of Estonia's international reputation and competitiveness.

Comparative Insights

Both the Czech Republic and Estonia demonstrate a commitment to cybersecurity through their regulatory frameworks, with each country's approach reflecting its specific context and challenges. The Czech Republic's strategy is characterized by a strong emphasis on protecting critical infrastructure and integrating cybersecurity within its national security framework. In contrast, Estonia's regulatory environment is shaped by its digital-first society, with a focus on safeguarding its e-governance ecosystem and enhancing the resilience of its digital services and infrastructure.

Despite these differences, both countries share common ground in their adherence to EU cybersecurity directives and their active engagement in international cybersecurity dialogues. This alignment ensures that both the Czech Republic and Estonia not only contribute to but also benefit from the collective cybersecurity initiatives and intelligence sharing within the EU and beyond.

The comparison between the Czech Republic and Estonia's cybersecurity regulatory environments highlights the diversity of approaches within the EU, underscoring the importance of national context in shaping cybersecurity policies and practices. It also illustrates the dynamic interplay between national priorities and EU-wide cybersecurity objectives, fostering a collaborative approach to addressing the complex challenges of digital security in the 21st century.

3.1.3 Funding Sources

The cybersecurity research and innovation (R&I) ecosystems within both the South Moravian Region and Estonia are bolstered by a comprehensive array of funding sources. These sources encompass European Union initiatives, detailed national and regional programs, substantial private-sector investments, and strategic public-private partnerships (PPPs). This multifaceted funding framework is essential for driving forward innovations, fostering collaborations across sectors, and enhancing the cybersecurity posture of both nations.

European Union Funding Programs

Both the South Moravian Region and Estonia benefit from Horizon Europe and the Digital Europe Programme, which are pivotal EU funding mechanisms that support collaborative research projects and capacity building in cybersecurity across member states. Horizon Europe and the Digital Europe Programme significantly benefit cybersecurity R&I in both countries. Horizon Europe facilitates collaborative research projects that span the continent, focusing on developing cutting-edge cybersecurity technologies and methodologies. The Digital Europe Programme, meanwhile, aims to boost the digital competencies of the European economy and includes a strong emphasis on building cybersecurity capacities to safeguard Europe's digital infrastructure and services.

National Funding in the Czech Republic

The Czech Republic's approach to funding cybersecurity R&I is characterised by a rich diversity of national programs:

- **Security Research Program by the Ministry of Interior**: Specifically aimed at enhancing the nation's cybersecurity defences, this program supports R&D projects that address national security challenges, including cyber threats.
- **Grant Agency and Technology Agency**: These agencies play a pivotal role in funding scientific research and technological innovation within the cybersecurity domain, encouraging projects that contribute to both national security and international cybersecurity efforts.
- **Ministry of Education and Ministry of Industry and Trade**: Through various initiatives, these ministries allocate funds to bolster the cybersecurity sector's infrastructure and workforce, aiming to enhance the Czech Republic's cybersecurity capabilities and competitiveness.
- **Private Sector Funding and Venture Capital**: The Czech cybersecurity ecosystem benefits from the private sector's active involvement, including sector-specific investments and venture capital. This funding is vital for startups and SMEs focusing on innovative cybersecurity solutions, facilitating their growth and market entry.
- **Financial Support for Third Parties (FSTP)**: Managed by the National Coordination Centre (NCC) under NÚKIB, this funding mechanism supports smaller projects and initiatives, enhancing the Czech Republic's integration into EU-wide cybersecurity initiatives and fostering collaboration across member states.

Regional Funding in the South Moravian Region

In addition to national programs, the South Moravian Region provides targeted support for cybersecurity innovation:

- **Regional Administration and South Moravian Innovation Centre (JIC)**: These entities offer grants for projects that contribute to the regional cybersecurity innovation ecosystem, particularly supporting early-stage development and commercialisation efforts.
- **University Funding**: Academic institutions in the region, such as Masaryk University, allocate funds to research teams and for the development of proof-of-concepts. This internal funding mechanism is crucial for advancing academic research in cybersecurity and translating research findings into practical applications.

Funding Sources in Estonia

Estonia's funding landscape mirrors its status as a digital-first nation, with a strong emphasis on supporting cybersecurity R&I.

In Estonia, national funding for cybersecurity-related research and development comes from several key sources, reflecting a diverse approach similar to that what is seen in the Czech Republic. Primary national funding sources for cybersecurity R&I in Estonia are:

- **Estonian Research Council (ETAg):** The Estonian Research Council provides competitive grants for scientific research, including cybersecurity. It supports various research projects aimed at enhancing national cybersecurity capabilities and fostering innovation in the field;

- **Ministry of Education and Research:** This ministry allocates funding to support higher education institutions and research organizations involved in cybersecurity R&I. Its initiatives aim to improve Estonia's cybersecurity infrastructure and advance its technological expertise;
- **Ministry of Economic Affairs and Communications**: The Ministry of Economic Affairs and Communications funds projects related to digital innovation and cybersecurity. It plays a significant role in supporting national strategies and initiatives that enhance the cybersecurity sector's development;
- **Information System Authority (RIA)**: RIA is responsible for the development and implementation of national cybersecurity policies, and they are also managing funding for various cybersecurity initiatives. This includes grants for projects that improve national security and resilience against cyber threats;
- **Private Sector Investments**: The Estonian cybersecurity ecosystem benefits from investments by private companies and venture capital firms. These funds are crucial for supporting startups and innovative solutions in the cybersecurity sector, contributing to the growth and international competitiveness of Estonian cybersecurity ventures;
- **Small Grants for Innovation**: The Cyber Accelerator Program for 2023-2024, managed by the National Coordination Centre (NCC-EE) and implemented by Tehnopol, has concentrated on introducing innovative cybersecurity products to the market. It has provided small grants without requiring equity in return.

These funding sources collectively support Estonia’s efforts to advance its cybersecurity R&I landscape, contributing to both national and international cybersecurity initiatives.

Comparative Insights and Synergies

The Czech Republic and Estonia exemplify how a combination of EU, national, regional, and private funding sources can collectively support a robust cybersecurity R&I ecosystem. While both countries benefit from EU initiatives for collaborative research and capacity building, their national and regional programs are specifically tailored to address unique cybersecurity challenges and priorities. The Czech Republic places a significant emphasis on national security and infrastructure protection, supported by a comprehensive suite of funding programs, including contributions from the private sector and private-public partnerships.

Estonia, with its pioneering digital government framework, prioritises funding that enhances the security and resilience of its digital infrastructure, also leveraging private investments and PPPs to foster innovation in cybersecurity.

This layered approach to funding not only facilitates a broad spectrum of R&I activities within the cybersecurity domain but also encourages collaboration among academia, industry, and government entities. By leveraging these diverse funding sources, the Czech Republic and Estonia enhance their national cybersecurity capabilities, contributing to the EU's collective security efforts and fostering innovation within their digital economies.

3.1.4 R&I Support Structures & cross sectoral cooperation

Research and Innovation (R&I) support structures play a pivotal role in the cybersecurity ecosystems of the South Moravian Region and Estonia. These structures, ranging from technology parks and innovation hubs to academic centres and public-private partnerships, provide the essential scaffolding for nurturing innovation, facilitating collaboration, and accelerating the transfer of research findings into market-ready solutions. This section explores the R&I support structures that bolster the cybersecurity landscapes in both countries, highlighting their contributions to fostering a vibrant and resilient cybersecurity sector.

South Moravian Region: A Network of Collaborative Innovation

In the South Moravian Region, the cybersecurity R&I infrastructure is characterized by a comprehensive network of support structures designed to stimulate innovation and collaboration:

- **Technology Parks and Innovation Hubs**: These spaces offer a conducive environment for startups and established companies to develop and refine their cybersecurity solutions. They provide access to state-of-the-art facilities, networking opportunities, and business services that are crucial for growth and development. Key role plays Cybersecurity Innovation Hub, which is a member of the European Digital Innovation Hubs (EDIH) Network and supports the implementation of cybersecurity innovation in both small and medium companies as well as in public institutions.
- **Cybersecurity Hub:** This non-profit initiative represents a joint venture among Masaryk University, Brno University of Technology, and Czech Technical University. The Cybersecurity Hub is designed to facilitate cooperation between universities and partners in the industry and public sector. It offers professional training in cybersecurity, coordinates projects aimed at building Quantum Communication Infrastructure (QCI) and chip design centres, and operates both the Cybersecurity Innovation Hub and the National Coordination Center in collaboration with the National Cyber and Information Security Agency (NÚKIB). This structure is pivotal in bridging the gap between academic research and practical, industry-relevant cybersecurity solutions.
- **Cyber Campus:** Situated in Brno, the capital of the South Moravian region, the Cyber Campus concept serves as a centre for cooperation among a diverse array of stakeholders. This includes public institutions such as the National Cyber and Information Security Agency, judicial institutions, the Supreme Public Prosecutor's Office, the Data Protection Authority, and the Military Intelligence with its Cyber Defense Center. The campus also brings together industry players like RedHat, Codasip, Avast, SolarWinds or Oracle, as well as research and education institutions, including Masaryk University, Brno University of Technology, Mendel University in Brno, University of Defence, and the Academy of Sciences. Technology parks such as CERIT and CERIT II, along with key industry organizations like the Network Security Monitoring Cluster and the Industry 4.0 cluster and non-profits like Czechitas, are integral parts of this ecosystem. The Cyber Campus exemplifies a comprehensive approach to fostering collaboration across sectors, enhancing the region's cybersecurity capabilities.

- **South Moravian Innovation Center (JIC):** Located in Brno, JIC holds the prestigious EBN certification from the European Business and Innovation Centres Network, which connects business and innovation centres internationally. JIC supports firms and startups at various development stages with four distinct programs: JIC ENTER for conceptual phase support, JIC STARCUBE for international acceleration, JIC MASTER for expansion to global markets, and JIC PLATINN for established companies. Established by the South Moravia region and key regional partners, including universities, JIC plays a critical role in nurturing innovation and facilitating the growth of the cybersecurity sector.
- **Academic and Research Institutions:** Universities and research institutes in the Czech Republic, such as Masaryk University and Brno University Technology, are at the forefront of cybersecurity research. These institutions not only contribute to advancing the knowledge frontier in cybersecurity but also play a key role in training the next generation of cybersecurity professionals.
- **Public-Private Partnerships (PPPs):** PPPs in the Czech Republic facilitate collaboration between the government, academic institutions, and the private sector, driving the development and implementation of innovative cybersecurity solutions. These partnerships leverage the strengths of each sector to address national cybersecurity challenges effectively.
- **National Cyber and Information Security Agency (NÚKIB):** As the central administrative body for cybersecurity in the Czech Republic, NÚKIB coordinates national cybersecurity efforts, including R&I activities. It acts as a bridge between government policy, academic research, and industry needs, ensuring that R&I initiatives align with national security objectives.

Estonia: Digital Innovation at the Forefront

In Estonia, the cybersecurity research and innovation infrastructure is characterized by a network of collaborative and supportive structures designed to foster innovation and partnership. Estonia's R&I support structures are deeply integrated into its digital-first society, emphasising the development of secure digital services and infrastructure:

- **Technology Parks and Innovation Hubs**: Estonia is home to various technology parks and innovation hubs that provide an ideal environment for cybersecurity startups and established companies. These spaces offer facilities, networking opportunities, and business services essential for growth. Notable examples include the **Tehnopol Science and Business Park** and **Tartu Science Park. Tehnopol Science and Business Park** is one of the largest science parks in the Baltic region, and it is a key player in Estonia's R&I ecosystem, supporting technology companies and startups, including those in the cybersecurity sector. It offers a range of services from incubation and acceleration programs to networking and advisory services. **Tartu Science Park** is also a prominent science park in Estonia, that is a vital component of the country's research and innovation ecosystem, providing essential support to technology firms and startup ventures, including those specialising in cybersecurity. Offering a diverse array of services ranging from incubation and acceleration programs to networking opportunities and advisory services, Tartu Science Park plays a crucial role in fostering innovation and growth within the region's technology sector. Another example is **StartUp Estonia** - a governmental initiative within the Estonian Business and Innovation Agency that works with different stakeholders to connect various sectors with the startup community. The Startup Estonia program is funded by the European Regional Development Fund, and it connects startups with various funding sources, including venture capital, grants, and accelerator programs. This support is vital for cybersecurity startups looking to develop and bring new technologies to the market.

- **Academic and Research Institutions**: Estonian universities, such as the **University of Tartu (UTartu)** and **Tallinn University of Technology (TalTech)**, play a crucial role in the R&I support structure by conducting cutting-edge research and offering specialized cybersecurity programs. These institutions foster an environment of academic excellence and innovation, significantly advancing cybersecurity knowledge and training the next generation of experts through their programs and research initiatives. Other universities, although not directly focused on cybersecurity, are nonetheless involved in related areas. For example, **Tallinn University** does not currently have a dedicated research group on cybersecurity. However, there are researchers whose work is related to cybersecurity, and previous research has addressed topics such as Digital Safety. **The Estonian Business School** also contributes to the field through the work of professors who have supervised several PhD researchers and published research papers on cybersecurity topics.
- **Estonian Research Council (ETAg):** ETAg provides grants and strategic support to research projects and initiatives, ensuring that Estonian research contributes to the global cybersecurity landscape.
- **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE):** The CCDCOE, based in Tallinn, Estonia, is a leading international military organisation that contributes significantly to cybersecurity research, education, and training. Established to support NATO and its member nations, the CCDCOE plays a crucial role in enhancing cyber defense capabilities and fostering international cooperation in addressing cyber threats.
- **CR14:** CR14 is a government-owned (established by the Estonian Ministry of Defence) and operated entity dedicated to advancing cybersecurity research and development. Serving both domestic and international partners across the private and public sectors, CR14 plays a pivotal role in enhancing global and national cybersecurity capabilities. Since 2014, CR14 has been responsible for developing and maintaining the NATO Cyber Range, a key resource for simulating and testing cyber defense strategies. Additionally, CR14 provides Host Nation Support to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), contributing to its mission of strengthening NATO's cybersecurity posture.

The Estonian National Coordination Centre (NCC-EE): NCC-EE of the European network of cyber security competence centres (NCC) is performed by the Research and Development Coordination Department of RIA. The aim of the centre is to promote the development of Estonian and European cyber security industry, technology, and research. NCC-EE is working closely with other European National Coordination Centres, as well as with the European Cybersecurity Competence Centre (ECCC).

Comparative Insights

Both the Czech Republic and Estonia have developed robust R&I support structures that cater to the diverse needs of their cybersecurity ecosystems. While the Czech Republic emphasises a comprehensive network of innovation hubs, academic institutions, and PPPs to drive collaborative research and development, Estonia leverages its digital-first approach to foster innovation in e-governance and cybersecurity, supported by a mix of science parks, international centres of excellence, and academic research.

These support structures not only facilitate the advancement of cybersecurity technologies and practices but also ensure that both countries remain at the forefront of addressing emerging cyber threats. By fostering collaboration across government, industry, and academia, the Czech Republic and Estonia enhance their resilience against cyber threats and contribute to the broader European and global cybersecurity efforts.

3.1.5 Key Stakeholders

Identifying and understanding the roles of key stakeholders within the cybersecurity research and innovation (R&I) ecosystems of the Czech Republic and Estonia is crucial for fostering effective collaboration and driving forward the development of robust cybersecurity solutions. These stakeholders, encompassing government agencies, academic institutions, industry players, and non-governmental organisations, contribute diverse perspectives, expertise, and resources to the cybersecurity domain. This section outlines the key stakeholders in both countries, highlighting their contributions and roles in enhancing cybersecurity capabilities and resilience.

Key Stakeholders in the South Moravian Region

- **Government Agencies**: The National Cyber and Information Security Agency (NÚKIB) stands out as a central figure, coordinating national cybersecurity efforts and policies. The region also hosts some other key government agencies and institutions like the Data Protection Office, Prosecutor General’s office, Military intelligence, key higher Judicial authorities, etc. Other important governmental stakeholders include the Ministry of Interior, responsible for the Security Research Program, and the Ministry of Industry and Trade, which supports industry collaboration and innovation. Cybersecurity research is also supported at the level of regional government, which operates its own Security Operations Center and offers support and funding to local governments and institutions in the area of cybersecurity.
- **Academic Institutions**: Universities such as Masaryk University and Brno University of Technology are pivotal in conducting cutting-edge cybersecurity research and developing the next generation of cybersecurity professionals. They also cooperate with other key research and education centres in the region, like the University of Defence or the Academy of Sciences. These institutions often collaborate with industry and government on R&I projects.
- **Industry Players**: The South Moravian Region hosts a vibrant mix of global IT companies and innovative startups. Notably, companies like RedHat, Oracle, AT&T, SolarWinds or Honeywell have established significant development centres in the region, contributing to its reputation as a hub for both IT innovation. Their involvement

in R&I activities, often in partnership with academic institutions, drives innovation and ensures that research outcomes have practical applications.

- **Innovation Hubs and Clusters**: The South Moravian Innovation Center (JIC) and technology parks such as CERIT facilitate collaboration between startups, established companies, and researchers, providing essential support for the commercializ’sation of cybersecurity innovations.

Key Stakeholders in Estonia

Estonia’s cybersecurity ecosystem is supported by a network of key stakeholders. These include government agencies, academic institutions, and industry players, each of which contributes to the country's strong cybersecurity capabilities and innovative research environment.

- **Government Agencies**: Estonia’s cybersecurity landscape is shaped by several key government agencies. **The Information System Authority (RIA)** is central, responsible for Estonian cybersecurity and critical infrastructure protection. The **Ministry of Economic Affairs and Communications** oversees national cybersecurity policies and initiatives, while the **Ministry of Defence** manages cyber defense activities, including those related to the **Estonian Defence Forces**. The Cybercrime Unit (C3EE) in the Central Criminal Police, as well as the **Estonian Internal Security Service** (KAPO) and **Estonian Foreign Intelligence Service** (VLA) also play a crucial role in safeguarding national security against cyber threats.
- **Academic Institutions:** As previously mentioned, the University of Tartu and Tallinn University of Technology are at the forefront of cybersecurity research in Estonia, offering specialized programs and engaging in international R&I collaborations. Their work contributes significantly to Estonia's reputation as a leader in digital and cybersecurity innovation. Additionally, the Estonian Academy of Security Sciences plays a crucial role in addressing cybersecurity issues.
- **Industry Players**: Estonia's vibrant industry ecosystem, featuring companies like **Guardtime, Cybernetica, CybExer Technologies, Cybers, SK ID Solutions** (etc.), is renowned for pioneering solutions in digital identity, blockchain technology, and e-governance. These companies are integral to the development and deployment of secure digital services. Furthermore, significant IT service providers such as Telia, Nortal, and BCS (etc.) also play a crucial role in maintaining robust cybersecurity measures in their operations and offerings.
- **Non-Governmental Organisations:** Several NGOs are also pivotal in Estonia's cybersecurity landscape. For example, organizations like the Estonian Union for Child Welfare, with their Targalt Internetis project, focus on child protection and internet safety. The Cyber Defence Unit of the Estonian Defence League plays an essential role in national cyber defense. Cluster organizations such as the Estonian Association of Information Technology and Telecommunications (ITL) and the Banking Association (Pangaliit), along with ISACA Estonia Chapter, contribute to collaborative efforts in cybersecurity, enhancing both public awareness and industry standards.

Cross-sectoral and International Collaboration

Both the Czech Republic and Estonia benefit from a dynamic interplay among key stakeholders within their cybersecurity ecosystems. This collaboration extends beyond national borders, involving participation in EU initiatives, international research projects, and global cybersecurity forums. Such engagement not only enhances domestic cybersecurity capabilities but also contributes to international efforts to combat cyber threats.

Conclusion

The cybersecurity ecosystems of the Czech Republic and Estonia are characterized by the active involvement of a wide range of stakeholders, each contributing unique expertise and resources to the collective effort of securing cyberspace. Government agencies provide policy direction and support, academic institutions contribute to research and talent development, industry players drive innovation and commercialisation, and innovation hubs and clusters facilitate collaboration and knowledge exchange. Together, these stakeholders form the backbone of robust and resilient cybersecurity ecosystems, capable of addressing current challenges and anticipating future threats.

3.2 Analysis of CHESS Challenge Areas

This section focuses on specific challenge areas that are critical to advancing the field of cybersecurity research and innovation (R&I). These challenge areas represent the cutting-edge of cybersecurity efforts, addressing both current threats and anticipating future vulnerabilities. This section aims to dissect these areas in detail, exploring the dynamics of stakeholder cooperation, identifying best practices, and conducting a SWOT analysis to uncover strengths, weaknesses, opportunities, and threats inherent to each area.

The cybersecurity landscape is continuously evolving, with new threats emerging as technology advances. To stay ahead, focused attention on key challenge areas is essential. These areas include:

1. **Internet of Secure Things (IoST)**: As the Internet of Things (IoT) continues to expand, securing the myriad of connected devices becomes increasingly critical. The IoST challenge area focuses on developing robust security protocols, standards, and solutions to protect IoT devices and networks from cyber threats.

2. **Security Certification**: This area addresses the need for standardised security certifications that can provide assurances of security levels for products, systems, and services. Security certification plays a crucial role in building trust among users and is vital for the adoption of new technologies.

3. **Verification of Trustworthy Software**: Ensuring software can be trusted is paramount in a digital world. This challenge area concentrates on methods and tools for verifying the security and reliability of software, including formal verification techniques and automated testing tools.

4. **Security Preservation in Blockchain**: As blockchain technology finds applications beyond cryptocurrencies into areas like supply chain management and identity verification, ensuring its security is paramount. This challenge area explores the unique security challenges posed by blockchain technologies and seeks innovative solutions to address them.

5. **Post-Quantum Cryptography**: With the advent of quantum computing, current cryptographic standards are at risk. Post-quantum cryptography focuses on developing new cryptographic algorithms that are secure against the potential capabilities of quantum computers.

6. **Human-Centric Aspects of Cyber-security**: It has been well recognised that the effectiveness of cyber-security is highly dependent on the human-centric aspects of cyber-security, both in terms of professionals and end-users of technologies. This challenge area focuses on cyber-security training and usable security.

For each challenge area, this analysis will provide a general description, highlighting the significance, current initiatives, and the state of R&I in South Moravia and Estonia. Key stakeholders involved in these areas will be identified, including their roles, how they collaborate, and the impact of their work. This section will also showcase examples of good practice, offering insights into successful strategies and initiatives that could serve as models for further development.

A SWOT analysis for each challenge area will offer a concise overview of the internal and external factors influencing the sector. This analysis aims to identify actionable insights that stakeholders can leverage to enhance cybersecurity R&I efforts, foster collaboration, and address the unique challenges and opportunities presented by each area.

Through this detailed exploration of challenge areas, this section seeks to contribute to a deeper understanding of the specific domains within the cybersecurity ecosystem that require focused attention and collaborative effort to ensure the security and resilience of digital infrastructures in South Moravia, Estonia, and beyond.

3.2.1 Internet of Secure Things

General Description

Many research institutions and industries worldwide extensively study the Internet of Secure Things (IoT). The security in IoT solutions has often been developed and progressed by global technology giants such as Intel, Google, Thales, Microsoft, Samsung, Apple, Gartner, ARM, GE, Arduino, Infineon, NXP, AMD, Cisco, Siemens, etc. Nevertheless, many regional SMEs contribute significantly with narrow and specific IoST solutions and products. In CA1, “Internet of Secure Things (IoST)”, CHESS partners aim to address open research challenges in this field and focus more on cooperation with regional SMEs. Standard cybersecurity trends in IoST usually focus on cost-efficient security (balanced cybersecurity), agility and other emerging challenges, including post-quantum transition, robustness and following complex thread and business models, certification and compatibility, and privacy-preserving protection for users of IoST services across various sectors such smart transportation, e-healthcare, smart industry, innovative city services, smart homes, smart grids, etc. Concretely, CA1 pays attention to the emerging sub-field of IoST, ITS (Intelligent Transportation Systems), that connects users, vehicles, roadside units, providers' systems, and other parties in the environment. There are many global pioneers in the ITS industry, such as Waymo, BOLT, Tesla, etc., but we instead aim at SMEs in both regions that focus on concrete systems and solutions.

Overall, long-term challenges and open research topics are deploying advanced cryptographic schemes into constrained devices and solutions used in IoT and ITS. The combination of quantum-resistance, decentralised security and privacy-preserving solutions, robustness and agile cryptography will be essential in future IoST/ITS systems. Creating privacy-preserving and secure IoT/ITS applications based on modern cryptography and security methods is also a long-term goal of CA1.

Artificial intelligence/machine learning (AI/ML) is getting more and more attention in the IoST domain. They are applied across domains (automated systems and technology, robotics, self-driving cars, finance, healthcare, etc.), where stakeholders and systems communicate sensitive data and decisions. One can apply AI/ML methods for <u>defensive</u> security. They can determine security risks, threats and vulnerabilities, including Intrusion detection, Detection of malicious objects in documents and websites, Detection of malicious activities in the network, etc. AI/ML methods can be used for offensive security. Examples of offensive AI/ML include evading authentication controls, autonomous/ automatic movement in attacks, enhancement of identity theft, etc.

The AI/ML applications should also be protected against malicious activities and security threats. Security attacks on AI/ML systems could be classified as poisoning and evasion attacks. AI/ML risk mitigation strategies are data modification and model modification. The data modification (e.g., adversarial training, data randomisation, etc.) addresses the training dataset during training, changing, or testing stages. Model modification (e.g., regularisation, defensive distillation, etc.) addresses changing the ML models. In the IoST domain, AI/ML systems analysis is challenging and could be seen as a future research direction in CA1.

Key Stakeholders

Listing and description of the main stakeholders involved in (and/or relevant to) each challenge area, focusing on their roles, contributions, and collaborations.

Key Stakeholders in Estonia

Academia:

- **University of Tartu Institute of Computer Science**
  - **Information Security Research Group** (infosec.cs.ut.ee) conducts research and teaching in the field of information security with an emphasis on secure system design and requirements engineering. The group is researching information security risk management, personal data management, and privacy leakage management in IoST, intelligent transportation systems and blockchain-based applications. This group is involved in the CA1 activities.

Other research groups which potentially can contribute or benefit from the CA1 research activities:

  - **Applied Cyber Security Group** (acs.cs.ut.ee) - perform research in cyber security, evaluating the security of the technology solutions used in our everyday life. The focus is directed towards solutions with significant public interest used in Estonia (e.g., electronic, digital signatures, internet voting and similar topics).
  - **Cryptography Research** Group (crypto.cs.ut.ee) conducts research into cryptography, in particular in Zero knowledge and zk-SNARKs, applications of ZK (blockchain, verifiable computation, e-voting, etc.), multi-party computation, and others.
  - **Autonomous Driving Lab** (adl.cs.ut.ee) (i) evaluates the current state of autonomous driving in terms of readiness for production, (ii) performs research in data-driven autonomous driving and mobility technologies, (iii) educates the future workforce for the up-and-coming autonomous driving industry.

- **Tallinn University of Technology** (TalTech):
    - Centre of Digital Forensics and Cybersecurity (taltech.ee/en/centre-for-digital-forensics-cyber-security) aims to raise the competence of Estonian digital forensics and cyber security through education, research and development, focuses on the relevant actions according to Estonian national cyber security strategy, cooperates and prepare for technological interchange with other relevant research fields. The centre is involved in the CHESS project but is involved in different challenge areas. CA1 could potentially cooperate on the research and teaching activies in the future.

Industry:

- **Cybernetica** (cyber.ee) performs world-class research, analyses complex systems, provides security-y-design solutions and researches public key infrastructure (PKI), cryptographic protocols, post-quantum cryptography with a focus on IoST systems and infrastructure, and many others. Cybernetica contributes to the CA1 activities.

Other potential organisations which can involve or benefit from the CA1 research and teaching activities:

- CybExer Technologies (cybexer.com) delivers digital twin-based testing and training environments that equip organisations to achieve cyber excellence. Such a platform enables organisations to anticipate and prepare for cyber challenges, meaning their cyber capabilities are primed when needed.
- In the IoST field, other relevant cooperation might be attempted with AuveTech (https://auve.tech), and Clevon (clevon.com) in the vehicle teleoperation; CityBee (citybee.ee/en/) and Bolt Drive (bolt.eu/et-ee/drive/) in the car-sharing scenarios; AIRE association (aire-edih.eu/en/) in the automatic systems and technology, application of the AI/ML method; Nortal (nortal.com), Playtech (www.playtech.ee) and other companies.

Other regional players in Estonia:

- Estonian Information System Authority (RIA) (https://www.ria.ee)
- City of Tartu (https://tartu.ee/en/citycouncil)
- Cyber Defence Unit of the Estonian Defence League (https://www.kaitseliit.ee/en/cyber-unit)
- The International Centre for Defence and Security (https://icds.ee/)
- Estonian Association of Information Technology and Telecommunications (https://itl.ee/en/)
- Foundation CR14 (https://cr14.ee/)
- Cyber Command (Estonian Defence Forces) (https://mil.ee/en/landforces/cyber-command/)
- Startup Estonia (https://startupestonia.ee/focus-areas/cybertech)

- ISACA Estonia Chapter (https://www.eisay.ee)
- eGovernment Academy: National Cyber Security Index (https://ncsi.ega.ee)

Key Stakeholders in South Moravia

Academia:

- **Brno University of Technology (BUT)** – The Brno **Applied Cryptography and Security Engineering (AXE) Group** (www.axe.vut.cz) at Brno University of Technology deals with cybersecurity and cryptography. The group members are responsible for teaching, doing research in projects, conducting contractual research and raising awareness in cybersecurity, including IoST. In addition, there is a collaboration with the CyberGrid lab that is focused on applied cryptography and cybersecurity in industrial networks, smart grids, smart homes, etc., see https://www.cybergrid.cz/ (in Czechia).
- **Masaryk University (MU)** – collaboration in applied cryptography and system security, e.g. with Centre for Research on Cryptography and Security (CRoCS) (https://crocs.fi.muni.cz/), and with Lab of Software Architectures and Information Systems (LASARIS) (https://lasaris.fi.muni.cz/).
- **Cybersecurity Hub (CSH)** – collaboration in networking, interdisciplinary security fields, and regulations, see https://www.cybersecurityhub.cz/en
- **University of Defence** - might be interested in CA1, secure IoT technologies and embedded security.

Industry:

- CHESS partners, BUT especially, have cooperated with companies such as **IMA** (cooperation on development of secure car access control systems and car sharing applications in CZ, see https://www.ima.cz/en/grantove-projekty/prodatran-2/), **AZD** (secure telematic solutions in ITS for crossroads, https://www.azd.cz/en), **Honeywell** (securing HVAC systems, https://www.honeywell.com/us/en), **Magmio** (the hardware implementation of cryptography methods, https://www.magmio.com/), **Herman Systems** (the security in embedded devices and systems in ITS, https://www.herman.cz/en/).
- Furthermore, there are more industry partners in SM region which are dealing with IoST and are potentially open for cooperation on research tasks: YUNEX, BKOM, Proficomms, Resideo, NXP, CAMEA, DataFromSky (RCE), Tropic Square, Škoda Auto (Development dept.) and Digiteq Automotive.

The following examples describe how cooperation with industry partners can be focused. YUNEX – enhancing secure and privacy ITS technologies in their solutions; BKOM – application and testing secure and privacy ITS technologies. Proficomms – collaboration in telematics for ITS and secure IoT networks. Resideo (Honeywell), NXP – creating secure embedded and IoT systems. AMEA and DataFromSky (RCE) – deploying privacy preserving technologies in ITS. Tropic Square – creating secure embedded and IoT systems based on open secure chip. Škoda Auto (Development dept.) – designing and enhancing secure telematic solutions in ITS. Digiteq Automotive – enhancing tests in cybersecurity in automotive electronics.

Other regional players

- **NÚKIB** (https://nukib.gov.cz/en/) – feedback, review, discussion.
- **BRNO city** (https://en.brno.cz/business-science) – cooperation with Brno city in smart cities and ITS services. For instance, Brno city launched a small project Brno In Motion (https://brnoinmotion.cz/) that mapping modern transportation applications and services.

Relevant networks, organisations, institutions, and governmental institutions (national/EU):

- European Cybersecurity Competence Centre (ECCC) (https://cybersecurity-centre.europa.eu/)
- European Cyber Security Organisation (ECSO) (https://ecs-org.eu)
- European Network and Information Security Agency (ENISA) (https://www.enisa.europa.eu)
- GSMA - a global organisation unifying the mobile ecosystem (gsma.com)

Relevant national or EU/international projects:

Past:

- CyberPhish: (https://cyberphish.eu)
- SPARTA: (https://www.sparta.eu)
- CyberSec4Europe: (https://cybersec4europe.eu)
- Concordia: (https://www.concordia-h2020.eu)
- ECHO: (https://echonetwork.eu)
- SECUREIoT H2020 project https://secureiot.eu/
- SerIoT H2020 project https://cordis.europa.eu/project/id/780139

Ongoing:

- SOCCER: Developing and deploying SOC capabilities for the academic sector - teamwork of Universities and RTOs in the CEE region
- CHAISE: Blockchain skills for Europe (relevant for CA4, education of Blockchain Technology), https://chaise-blockchainskills.eu
- C-ROADS: deployment activities of cooperative intelligent transport systems (C-ITS) across Europe, https://www.c-roads.eu/platform.html

National/regional policies/strategies/regulations:

- E-ITS https://eits.ria.ee

Major European policy/strategy/regulation for the area:

- ETSI standards for ITS[1]
- ETSI standards for recommendations and guidance on IoT security and privacy[2]
- ENISA Guidelines for Securing the Internet of Things[3]
- GSMA IoT SAFE: This is a set of security guidelines and assessment tools for the IoT supply chain, developed by the GSMA[4]

Cooperation and Best Practices

- At the University of Tartu, the InfoSec research group and ADL have several ongoing cooperations to explore the security of autonomous vehicles [https://adl.cs.ut.ee/research/research-areas/security].
- Previously, Cybernetica and the University of Tartu (also including Infosec) were collaborating on the project on Novel tools for Analyzing Privacy LeakageS (NAPLES) [https://cyber.ee/research/projects/naples].
- The city of Tartu, the University of Tartu, and CybExer Technologies signed a cooperation agreement to explore smart city mobility solutions using the cyber range technology. [https://cs.ut.ee/en/content/tartu-enhance-cybersecurity-smart-city-solutions]
- University of Tartu and the Estonian Information System Authority (RIA) cooperate on the project on analysis of cyber security risks and mitigation options for automated systems and technologies and the creation of educational videos.
- Previously, the Applied Cryptography and Security Engineering (AXE) group (the Brno University of Technology) and Information Security (InfoSec) research group (University of Tartu) collaborated in the SPARTA project on the privacy-preserving solution for vehicle parking services [5] and other initiatives.
- The AXE group currently cooperates with MU (CRoCS), NÚKIB and Czech Technical University in the long-term national cybersecurity project: Tools for AI-enhanced Security Verification of Cryptographic Devices (SecTools), and with NÚKIB, CESNET and Technical University of Ostrava in the project called Network Cybersecurity in Post-Quantum Era (NESPOQ) (https://www.nespoq.cz/).
- The AXE group also cooperated with various industrial partners in past, e.g., with IMA in national projects focused on applied cybersecurity: Modular System for Safe Data Collection in Industry 4.0, Legal and technical means of privacy protection in cyberspace, and with Magmio (former Netcope) in the projects: Cryptographic privacy protection in 100 GbE networks, Modular Hardware Accelerator for Cryptographic Operations. This collaboration of academy and industry enables the application of research results in practical products and services.

[1] https://www.etsi.org/committee/its

[2] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[3] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[4] https://www.gsma.com/iot/iot-safe/

[5] Dzurenda P, Jacques F, Knockaert M, Laurent M, Malina L, Matulevicius R, Tang Q, Tasidou A. 2022. Privacy-preserving solution for vehicle parking services complying with EU legislation. PeerJ Computer Science 8:e1165 https://doi.org/10.7717/peerj-cs.1165

- The InfoSec research group (University of Tartu) and the Masaryk University cooperate on designing forensic-ready risk aware software toolkit [6] .

Knowledge transfer needs and opportunities

Creating the matrix of security and privacy properties and priorities defined by stakeholders in IoST and ITS fields. Transfer of best practices and state-of-the-art cybersecurity approaches and cryptography tools into practice. This could include the following aspects:

- Design an IoST considering the need for interoperability with external systems and partners.
- When developing IoST systems, consider the usage of state-of-the-art measures and best practices (e.g., ones reported in academic publications).
- Collaborate with research institutions to help navigate state-of-the-art security and privacy countermeasures.

SWOT Analysis

Table 1: SWOT Analysis: Internet of Secure Things

Strengths	Weaknesses
• Good cooperation between different sectors (academia and businesses) • Good infrastructure	• Lack of cooperation with bigger international technology companies and SMEs from our regions necessary for potential future project
Opportunities	**Threats**
• Create new collaborations and growth of the research team thanks to new projects • Establish academia-public-private settings (inter-sectoral workshops, consultations) • Organise meetups/ seminars to access different sectors, potentially in English • Grow research teams • Establish collaboration with national foreign partners on design, optimisation and implementation of IoST solutions	• Financial dependency, project-based financing • Regional companies are less open for a research cooperation without a concrete common project

A comprehensive comparison of the Information Security and Privacy Management in Intelligent Transportation Systems is provided in the publication [7].

[6] Lukas Daubner, Martin Macak, Raimundas Matulevičius, Barbora Buhnova, Sofija Maksović, Tomas Pitner, Addressing insider attacks via forensic-ready risk management, Journal of Information Security and Applications, Volume 73, 2023, 103433, https://doi.org/10.1016/j.jisa.2023.103433

[7] M. Bakhtina, R. Matulevičius, L. Malina, “Information Security and Privacy Management in Intelligent Transportation Systems,” Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. xx, pp. xx–xx, 2024. Available: https://doi.org/10.7250/csimq.2017-xx.xx

3.2.2 Security certification

General Description

In the realm of cybersecurity, certification plays a crucial role in establishing trust and ensuring the robustness of digital infrastructures and technologies. Until recently, the Czech Republic lacked a comprehensive framework or infrastructure specifically dedicated to cybersecurity certification, with only some entities providing certification based on ISO27k scheme.

This situation is set to change dramatically with Czechia's anticipated participation in the European cybersecurity certification framework, a key component of the EU Cybersecurity Act. To facilitate this integration, the Czech Act on Cybersecurity has been amended, laying the groundwork for the implementation of cybersecurity certification within the Czech legal environment. This amendment assigns oversight of the certification mechanism to the National Cyber and Information Security Agency (NÚKIB), positioning it as the supervisory authority. Additionally, the Czech Institute for Accreditation is tasked with providing accreditation to relevant Conformity Assessment Bodies and Certification Laboratories, ensuring that certification processes adhere to stringent standards. Despite these significant steps forward, the process of establishing a fully operational certification framework has been relatively slow. This delay is attributed to the absence of available certification schemes and, consequently, the lack of dedicated funding to support these initiatives. The market demand is not clear as the European certification regulations and activities are not clear yet.

The National Cyber Security Act has established a baseline for managing information security (E-ITS), which RIA supervises. Another option to fulfil the regulation requirements is to be certified against ISO/IEC27001. ISO/IEC 27001 certifiers operating in Estonia are accredited by accreditation organisations located outside Estonia. Creating a national accreditation possibility is a work in progress. Holding the certification mechanisms is the responsibility of The Estonian Consumer Protection and Technical Regulatory Authority. Certification of Estonian information security baseline E-ITS implementation on the ISO/IEC 27001-based scheme is also under consideration.

The Estonian Centre for Standardisation and Accreditation currently has no certainty for the accreditation of evaluation of cyber products, services and processes because of the small size of Estonia and the lack of market demand, where it is easier to cooperate with other member states, including Czechia. However, at least it is planned to enable the organisation's ISMS certification accreditation.

Key Stakeholders

In Czechia, two key stakeholders emerge to enable the establishment and governance of the certification framework: the National Cyber and Information Security Agency (NÚKIB) and the Czech Institute for Accreditation. NÚKIB, with its newly assigned oversight responsibilities, is set to play a crucial supervisory role in the cybersecurity certification mechanism. The Czech Institute for Accreditation complements this by accrediting Conformity Assessment Bodies and Certification Laboratories, a critical step in maintaining the integrity and reliability of the certification process.

Several CHESS partners – Masaryk University, Brno University of Technology, Cybersecurity Hub and NÚKIB are key players in the Czech cybersecurity certification-related research. Some undertake to investigate options for the development of sound certification methodologies; some develop tools to investigate both the certification ecosystem and the systems/products this system covers, and some undertake investigation of regulatory approaches.

The creation and successful implementation of a cybersecurity certification system in Czechia hinge on two significant factors: the availability of funding and the size of the certification market. These elements are instrumental in determining the scope, reach, and effectiveness of the certification framework. So far, the interest from organizations in becoming Conformity Assessment Bodies or Certification Laboratories has been limited, with only a handful expressing their intention to participate in this system. This cautious approach reflects the non-existent certification market in Czechia and underscores the importance of developing a robust, funded, and market-responsive certification ecosystem.

In Estonia, the Estonian Information System Authority (RIA) supervises and manages the Estonian Information Security Standard (E-ITS). The Estonian Consumer Protection and Technical Regulatory Authority holds the certification mechanism and participates in ENISA certification working groups. The Centre for Standardisation and Accreditation plans to start providing accreditation services for Estonian certification service providers to assess organisations and their processes' compliance with ISO/IEC 27001. The Ministry of Economic Affairs and Communications and the Estonian Foreign Intelligence service have also expressed interest in certification of different products.

Cooperation and Best Practices

In the Czech Republic, a notable best practice in the realm of cybersecurity cooperation and certification has emerged through the collaborative efforts of three leading universities: Masaryk University, Brno University of Technology, and Czech Technical University. These institutions have come together to establish the Cybersecurity Hub Institute (CSH), a pioneering initiative designed to play a critical role within the cybersecurity certification landscape. The CSH is expected to serve as a Conformity Assessment Body, aligning with both the European Union's Certification framework and the conformity assessment framework introduced by the EU Cyber Resilience Act. Another noteworthy best practice in the Czech Republic's approach to enhancing its cybersecurity certification infrastructure involves the strategic use of Financial Support For Third Parties (FSTP) by the National Coordination Centre.

Additionally, the collaboration between academia and relevant public institutions in developing new proposals, methodologies and tools for cybersecurity certification schemes represents an impactful best practice. A prime example of this collaborative effort is the initiative focused on the certification of smart electricity meters. This project sees energy companies joining forces with the Brno University of Technology, leveraging academic expertise and industry insights to address specific cybersecurity challenges associated with smart grid technologies. Another example is a research project of the Ministry of Interior in close collaboration with NÚKIB, where Masaryk University, Brno University of Technology, and Czech Technical University develop several tools to support the certification ecosystem.

Knowledge transfer needs and opportunities

- Creating a clear certification roadmap for cryptographic modules

- Creating a clear roadmap on how to achieve the requirements set by the recent EU legislation
- Hands-on trainings on security certification frameworks, such as the SCRUTINY framework developed by MUNI to automate verification of security products such as smartcards delivered to the end-user.

Training CA2 needs or would find beneficial
Interaction with industry – identification of values and demands
Proposal writing for junior researchers
Public speaking

Training CA2 can offer to the project partners (and beyond):
Regulatory frameworks (Czech, EU) for cybersecurity certification
Analyzing the Common Criteria and FIPS certification documents using seccerts

SWOT Analysis

The development and implementation of a cybersecurity certification framework in the Czech Republic, particularly with initiatives like the establishment of the Cybersecurity Hub Institute (CSH) and collaborative efforts for new certification schemes, present a clear opportunity. This analysis aims to identify the Strengths, Weaknesses, Opportunities, and Threats associated with these endeavours.

Table 2: SWOT Analysis: Cybersecurity Certification in Czechia

Strengths	Weaknesses
• **Established academic infrastructure based on research achievements**: The collaboration of leading universities (Masaryk University, Brno University of Technology, Czech Technical University) in forming the CSH leverages existing expertise and laboratory infrastructure, providing a strong foundation for certification activities. • **Collaborative ecosystem**: The cooperative model between academia, industry, and public institutions, exemplified by projects like the smart electricity meters certification or tools for security certification, fosters innovation and ensures that certification schemes are relevant and grounded in real-world needs.	• **Limited initial interest**: So far, only very few organizations have expressed interest in becoming Conformity Assessment Bodies or Certification Laboratories, indicating potential challenges in scaling the certification ecosystem. • **Lack of clear information by the industry:** The industry misses clear guidance for the EU certification regulations and cannot assess the needs for certification. • **Funding dependency**: The establishment and expansion of certification infrastructure heavily rely on available funding, including FSTP by the National Coordination Centre, which could limit growth if not adequately supported. • Lack of people with relevant skill sets
Opportunities	**Threats**
• **EU alignment**: Participation in the European cybersecurity certification framework opens avenues for Czechia to	• **Rapid technological evolution**: The fast pace of technological advancements may

influence EU-wide cybersecurity standards and practices, enhancing its stature and competitiveness in the digital market. • **Innovation and expansion**: The development of new certification schemes, such as for smart electricity meters, presents opportunities for Czechia to lead in niche areas of cybersecurity, potentially attracting more interest and investment in its certification services.	outstrip the development and implementation of certification schemes. • **Certification attempts to drive the market:** Overly complex system of certification demands could challenge the relevance and efficacy of the certification framework. • **International competition**: As other EU member states develop their certification infrastructures, Czechia faces competition in attracting organizations to its certification services, necessitating continuous innovation and improvement to remain attractive.

This SWOT analysis underscores the balanced view of the current state and future prospects of cybersecurity certification in Czechia. While there are clear strengths and opportunities that Czechia can leverage, addressing the identified weaknesses and threats is crucial for the successful establishment and growth of its cybersecurity certification ecosystem.

3.2.3 Verification of Trustworthy Software

General Description

This challenge area concentrates on developing and deploying methods for formal verification and analysis of computer software into industrial practice. More concretely, the activities are concentrated around three main priorities:

1. Making use of program analysis techniques to improve software development.
2. Developing a theory of composable cybersecurity protocols to offer visual accounts of organisational cybersecurity protocols understandable to non-experts.
3. Identifying practically motivated challenges for basic research not yet covered by existing methodologies.

The consortium combines the expert knowledge of researchers at FI MUNI, FIT BUT, and TalTech with the practical experience of leading companies in the region (RedHat, Cybernetica). This allows for establishing mechanisms for direct and efficient evaluation of theoretical concepts in industrial practice and specifying new research priorities based on the evaluation outcomes. The technology transfer is typically achieved via dedicated tools for software analysis/verification that are freely available also to other software companies in the region.

Key Stakeholders

The key stakeholders are research teams at FI MUNI, FIT BUT, and TalTech, and companies interested in applying formal methods in industrial practice (RedHat, Cybernetica). The academic teams concentrate on solving the relevant problems of fundamental research and implementing the newly discovered methods into working software tools. Industrial partners provide practical feedback and contribute to identifying the crucial deficiencies and missing functionality. This leads to modifying the current research priorities and setting new goals.

Cooperation and Best Practices

The main (and most efficient) tool for managing the cooperation among the team members are intensive informal contacts among the involved researchers and representatives. This allows for

- managing concrete technical tasks (such as implementing new functionality into a software tool) where several team members directly cooperate;
- redefining the priorities in the three main challenge areas on-the-fly and initiating new miniprojects withing these areas.

A broader publicity and impact is achieved by organizing annual open events (Industial Days) where the project’s results are presented in the form of summary talks and subsequently discussed with industrial representatives participating in these events.

Knowledge transfer needs and opportunities

- Evaluating software tools for technology transfer developed by the key stakeholders.

- Identifying the missing functionality and crucial limitations of state-of-the-art formal methods.

Training CA3 needs or would find beneficial, i.e. needs identified by Czech CHESS partners:

- Improving presentation skills for junior researchers.
- Learning the ways of achieving broader publicity of the results ("PR skills").

Training CA3 can offer to the project partners (and beyond):

- Using the existing tools for formal verification and analysis of software systems, identifying most appropriate technologies for solving concrete technical problems via technology transfer days and short-term staff exchange.

SWOT Analysis

Table 3: SWOT Analysis: Verification of Trustworthy Software

Strengths	**Weaknesses**
• Sufficient level of international cooperation • Good links between academia and industry	• Funding dependency, sufficient funding for PhD students and PostDocs missing
Opportunities	**Threats**
• More joint meetings involving academics and industrial representatives • Training in hard skills needed • Infrastructure missing: A reliable computational infrastructure involving GPUs would be beneficial	• Regional companies are less open to research cooperation without a concrete common project

3.2.4 Security Preservation in Blockchain

General Description

Blockchain technology is a decentralized and distributed ledger system. Its fundamental concept involves recording transactions across multiple computers in a way that is transparent, secure, and tamper-proof. Blockchain has the potential to revolutionize various industries by providing immutable records of transactions, enhancing transparency and security, reducing fraud, and streamlining processes. Its applications extend to supply chain management, healthcare, voting systems, identity verification, and more. Additionally, blockchain serves as a foundation for building trust in digital interactions and has the capacity to reshape the future of how we exchange value and information. In the CHESS project, under Security Preservation in Blockchain (CA4), we focus on developing secure applications by leveraging blockchain technology as a fundamental security enabler. Our focus extends beyond mere secure application development using blockchain; we delve into the intricate landscape of security challenges and threats inherent within blockchain architectures and blockchain-based applications. Through rigorous exploration and analysis, we aim to identify, understand, and mitigate potential vulnerabilities, ensuring that our blockchain solutions uphold the highest standards of security and resilience in the face of evolving cyber threats.

In Estonia, several global trends are shaping various sectors of the economy and society. Security and cybersecurity remain paramount, with a growing emphasis on protecting digital infrastructure and combating cyber threats. Estonia is at the forefront of blockchain technology, collaborative ecosystems, and smart infrastructure development, fostering a conducive environment for digital innovation and entrepreneurship. In Estonia, blockchain technology has been gaining significant traction in recent years, reflecting a broader global trend towards its adoption and implementation across various sectors. With its forward-thinking approach to digital innovation, Estonia has positioned itself as a hub for blockchain development and actively exploring the potential applications of blockchain in areas such as e-governance, cybersecurity, supply chain management, and digital identity verification (https://investinestonia.com/business-opportunities/blockchain/). Estonia also continues to witness a steady rise in blockchain-related startups, research initiatives, and collaborative projects. Other trends are emerging in Estonia as well, such as machine learning and artificial intelligence (ML/AI) stand out as significant trends in Estonia, spearheading innovation across diverse industries and fostering advancements in automation and predictive analytics. The country is witnessing a surge in the development and testing of autonomous vehicles and delivery robots, signalling a shift towards more efficient and sustainable transportation solutions. Additionally, Estonia's strong focus on data science and natural language processing is driving advancements in data analytics and language technologies. Business process management and human-computer interaction are evolving to streamline operations and enhance user experiences, while the startup ecosystem continues to thrive, attracting talent and investment to fuel further innovation and growth. These burgeoning trends often intersect with blockchain technology to drive innovation and efficiency across various operations.

Various groups in the Czech Republic and South Moravia region were developers and early adopters within Bitcoin ecosystem, later extended to a wider blockchain area with world-wide first mining pool established here in 2011 (Slush pool), the first world-wide hardware wallet build in 2013 (Trezor wallet by Satoshi Labs) or largest cryptocurrency ATM machines provider from 2014 (General Bytes) among others. Frequently, the strong focus was on open-source software and hardware (Trezor wallet), open protocols (Stratum, BIP39) or design of cryptographic chips (Tropic Square) to name a few. The generally high level of education, especially in STEM domains and technical competence in software and hardware development created a good environment for concepts transfer into practice. The existing industrial-academic cooperation help with knowledge transfer in both directions and informs also potential research topics tackled in this CA.

Estonia

Academic Institutions:

- **University of Tartu, Tartu, Estonia:** From University of Tartu, Institute of computer science (https://cs.ut.ee), three research groups are mainly focusing on security aspects in various application domains. (1) Information Security Research Group –

https://infose.cs.ut.ee, (2) Applied Cyber Security Group – https://acs.cs.ut.ee, and (3) Cryptography research – https://crypto.cs.ut.ee.

  - **Information Security Research Group** specializes research and teaching emphasis on secure system design and requirements engineering, information security risk management, personal data management, and privacy management, intelligent transportation systems and blockchain-based applications. This group is involved in the CA4 activities.
  - **Cryptography Research Group** conducts research in Zero knowledge proofs (ZKPs), applications of ZKPs (blockchain, verifiable computation, e-voting, etc.), multi-party computation, and others.
  - **Applied Cyber Security Group** focuses on electronic, digital signatures, internet voting. Both research groups are not affiliated with CA4; however, we have the opportunity to collaborate on research and leverage the findings of CA4.

- **Tallinn University of Technology:** Tallinn University of Technology and the University of Tartu collaborate on a joint curriculum in Cybersecurity through the Centre of Digital Forensics and Cybersecurity (https://taltech.ee/en/centre-for-digital-forensics-cyber-security), aimed at enhancing Estonia's digital competence. While our team is not currently involved in CA4 cooperation, we do oversee Master's students from this joint cybersecurity curriculum within the CA4 framework.

Industry:

- **Cybernetica** (https://cyber.ee) is a prominent cybersecurity firm based in Estonia, renowned for its expertise in analyzing complex systems and offering security-by-design solutions. Their research and development efforts span various domains, including cybersecurity, data exchange technologies, digital identity technologies, tax and customs systems, and surveillance systems. Notably, Cybernetica is actively collaborating on research initiatives within the CA4 project.

- **Guardtime** (https://guardtime.com/): Guardtime developed a blockchain-based system that can verify the correctness of data and processes. Our research is aligned in terms of blockchain for data security. Guardtime can use the results of our work to understand how blockchain can play a role in internet of vehicles to secure data transmitted from them. Under CA4, Guardtime is collaborating on Zero-knowledge proofs and their role in blockchain and blockchain-based applications.

Other companies that might use the research results from CA4:

- **Bolt OÜ** (https://bolt.eu)**:** Bolt is an Estonian mobility company that offers ride-hailing and micromobility rental.
- **Auve Tech OÜ** (https://auve.tech/): Creating innovative solutions that enable vehicles to operate autonomously, without the need for human intervention.

- **Starship Technologies** (https://www.starship.xyz/): Starship Technologies, an Estonian-based company, is at the forefront of developing autonomous delivery robots/vehicles.
- **Cleveron** (https://cleveron.com/): Cleveron, an Estonian company, specializes in the development and production of robotics-based parcel terminals tailored for the retail and logistics sectors.

These above listed companies are working on intelligent vehicles or robots equipped with Internet of Things (IoT) devices, sensors, smart devices to receive and transmit data. Our use case related to Internet of Vehicles (IoV) can show the integration of blockchain technology for developing a more secure, available and reliable system.

Other regional players in Estonia:

- **Estonian Information System Authority (RIA):** https://www.ria.ee/
- CybExer Technologies (https://cybexer.com/): CybExer employs the Digital Twins concept for security testing and training. Our research also introduces a Digital Twin-based solution that can potentially enhance Cyberex's capabilities. This portion of our work can be seamlessly integrated into Cyberex's framework.
- **Cybers OÜ** (https://cybers.eu/): Cybers is at the forefront of innovation, harnessing advanced technologies to integrate and implement security solutions across various domains. Our blockchain-based solution for predictive maintenance on the Internet of Vehicles can seamlessly expand their operational scope.
- **STACC OÜ** (https://stacc.ee/)

In CA4, various stakeholders play crucial roles, contributing to the advancement and implementation of innovative solutions. Academic institutions like University of Tartu and Tallinn University of Technology provide research expertise and academic rigor. Companies such as Cybernetica and Guardtime bring industry experience and technological capabilities to the table, with Guardtime's expertise in blockchain aligning closely with our research focus on data security. Additionally, companies like Bolt OÜ and Auve Tech OÜ, operating in the mobility and robotics sectors, stand to benefit from our research outcomes. For instance, these companies are working on intelligent vehicles or robots equipped with Internet of Things (IoT) devices to receive and transmit data. Our use case internet of vehicles can show the integration of blockchain for developing a more secure, available and reliable system. Regional players like the Estonian Information System Authority (aka Riigi Infosüsteemi Amet RIA), CybExer Technologies, Cybers OÜ, and STACC OÜ contribute to the ecosystem by offering expertise, resources, and potential integration opportunities for our solutions. For example, our Blockchain and Digital Twin-based solution complements CybExer’s security testing and training framework, while our blockchain-based predictive maintenance system aligns with Cybers' innovative approach to security solutions. Overall, collaboration among these stakeholders fosters synergies, accelerates technology adoption, and drives impactful outcomes in each challenge area.

South Moravia

Academic and Governmental Institutions:

- **Masaryk University:** Institute of Computer Science, Information Security Research Group and MUNI (CRoCS security laboratory at Faculty of Informatics, MUNI.)
- **FIT BUT** (https://www.fit.vut.cz/.en)**:** is relevant to blockchain-related topics with two research groups active in the domain. MUNI has established research contact with both.
- **NUKIB** (https://nukib.gov.cz/en/): NUKIB is relevant due to analysis of secure hardware implementations (part of CA4 investigating the usage of secure hardware in blockchains) and analysis of security certificates (relevant especially for CA2, but with overlap to CA4 due to utilization of cryptographic hardware). NUKIB and MUNI has long-term cooperation, where research outputs in the form of better tools, better methods, and more accurate analysis were utilized.

Industry:

- **Monet+** (https://www.monetplus.cz/) is a long-running company which delivered Czech eID identity documents, card-based payment solutions and mobile banking applications and cooperates with MUNI via industrial partnership including PhD student support in a domain of secure multiparty signatures and analysis of smartcards and hardware wallets.
- **TropicSquare** (https://tropicsquare.com/) (part of the team in Brno, otherwise is Prague-based company). Tropic Square produces its own open-hardware security chip with usage targeted for cryptocurrency hardware wallets and similar scenarios. FI cooperates in analysis of on-chip ECC implementation using FI-developed testing tools and random number generator assessment
- **Satoshi Labs** (https://satoshilabs.com/) (part of the team in Brno, otherwise is Prague-based company). They may utilize project outputs in future, possibly indirectly via the usage of secure chip produced by Tropic Square or improved guarantees of CoinJoin mixing protocol.

Relevant EU/international projects:

- CyberSec4Europe project No. 830929 (MUNI and other partners)
- ORCHIN project No. 101070008 (TropicSquare and partners)

Other regional players in South Moravia:

- **Infineon/NXP/G+D cryptographic chips manufacturers** – cooperation during responsible disclosure of vulnerabilities found.
- **SatoshiLabs and TropicSquare** – initial discussions about the usage of our tools for cryptographic implementation analysis.
- **Turing Institute** – AI data analysis – initial cooperation started (past contacts from secure multiparty signatures domain already existing).

Cooperation and best practices:

University of Tartu, **Cybernetica** from Estonia and **Queen's University Belfast in the UK** are jointly working on a research publication within the CA4 project, focusing on the topic of Predictive Maintenance of Vehicles using Digital Twins and Blockchain. The collaboration underscores the importance of international partnerships in advancing research and innovation, leveraging the expertise and resources of both institutions to address complex challenges in the domain of autonomous systems. This collaboration serves as a best practice, demonstrating the benefits of cross-border cooperation and interdisciplinary research approaches in driving impactful outcomes within the challenge area.

The **University of Tartu** is collaborating with **Brno University of Technology (BUT)** as part of the CA4, specifically focusing on a mini-project centered around blockchain for secure communication. This collaborative effort aims to explore the potential of blockchain technology in enhancing the security of Internet of Vehicles (IoV). By leveraging blockchain's decentralized and immutable nature, the project seeks to develop innovative IoV's solution that can address the challenges associated with secure communication, data integrity, authentication, and confidentiality.

Masaryk University is cooperating with **Tropic Square, CZ** on the analysis of open-source cryptographic chip with a focus on ECC implementation correctness and quality of truly random number generator.

Masaryk University is working jointly with researchers from **Turing Institute, UK** on usage of machine learning in analysis of privacy offered by CoinJoin protocols.

Masaryk University and **Monet+, CZ** cooperated for almost 20 years on join projects in analysis of secure hardware, usage of cryptographic smartcards and secure multiparty protocols suitable for computationally and memory restricted environments.

Knowledge transfer needs and opportunities:

- Blockchain research training for educating individuals on the fundamentals of blockchain technology, including its underlying principles, consensus mechanisms, and smart contract development.
- Entrepreneurship training within the blockchain space may focus on fostering innovation and enabling individuals to explore opportunities for blockchain-based startups or projects.

Training CA4 needs or would find beneficial:

- Training programs aimed at enhancing academic collaboration with companies and industries in the field of blockchain technology would be valuable.
- Providing guidance on time management and entrepreneurship training, focusing on strategies for selecting important tasks and effectively declining unimportant ones across different levels of work experience, catering to both PhDs and employees.
- Offering diverse training programs aimed at facilitating onboarding processes and enhancing expertise in various domains, addressing the unique needs and skill levels of individuals within the organization.

- Grant proposal writing.
- Deep work and zen training :)

Training CA4 can offer to the project partners (and beyond):

- University of Tartu organizing blockchain training workshop in MUNI.
- University of Tartu organizing blockchain training workshop in BUT.
- Masaryk University organizing Threshold cryptography demonstrator platform workshop (MeeSign).
- Masaryk university organizing workshop on usage of hardware wallets, multisig and privacy CoinJoin in Bitcoin ecosystem.

SWOT Analysis

Table 4: SWOT Analysis: Security Preservation in Blockchain

Strengths	Weaknesses
• **Grassroot knowledge in domain space**: Both Czechia (Satoshi Labs, Braiins, General Bytes...) and Estonia (Guardtime...) have large societal and entrepreneurial base with resulting knowledge transfer and base level of education in the domain space. • **Real-world applicability:** The high number of active companies and projects in the domain provides access to real-world problems to solve, data to analyze and opportunities to verify approaches proposed. • **Shared resources:** Collaborative work and projects can often benefit from shared resources, such as funding, facilities, and equipment, maximizing efficiency and reducing costs • **International collaborations:** Collaboration harness the combined expertise, resources, and networks of multiple stakeholders, leading to synergistic outcomes that may not be achievable individually. • **Research advancements and knowledge sharing:** Collaboration brings together individuals with diverse backgrounds, skills, and perspectives, fostering creativity, innovation, and holistic problem-solving approaches.	• **Immature state of ecosystem:** The rapid pace of technological developments and lack of established quality metrics results in a high fraction of unrealistic or even scam projects, companies and proposals. • **Low legal clarity**: The high pace of technological development naturally creates gap between products available and their legal implications like digital tokens nature (digital property vs. digital currency), taxation, requirements on KYC/AML rules, liability or participants. As a result, development may be hampered by unclear (future) legal status. • **Coordination challenges:** Coordinating activities, communication, and decision-making among multiple stakeholders can be complex and time-consuming, leading to inefficiencies and delays. • **Conflicting priorities:** Different stakeholders may have divergent goals, priorities, and expectations, potentially leading to conflicts, disagreements, and challenges in aligning interests. • **Governance issues:** Establishing clear governance structures, roles, and responsibilities is essential for effective collaboration, but governance issues such as decision-making bottlenecks can impede progress.
Opportunities	**Threats**

• **New cross-board and inter-sectoral links:** resulting in long-term quality cooperation within the projects. • **Lowering bureaucracy tasks** by utilizing experience from other countries. • Joint training sessions, seminars, and hands-on practical workshops (connecting business and academia). • **Access to specialized infrastructure:** Access to state-of-the-art laboratories, research facilities, and equipment to significantly enhance the quality and scope of our research. This is particularly important for projects that require specialized tools and resources, e.g., hardware-level security testing. • **Mentorship and guidance:** Guidance from experienced researchers or mentors can help shape research strategies, provide insights, and ensure research activities align with best practices. • **Public engagement support:** If the research aims to address societal issues, support for public engagement and dissemination of results is valuable for creating real-world impact. Sharing practical experience between countries.	• **Increased closeness of ecosystem** of secure hardware chips and resulting security by obscurity approach, lack of transparency of certification claims. Increased control and limitations over cryptographic platforms, especially cryptographic smartcards. • **Lack of low-level access** to hardware layers so newer algorithms are hard to implement (especially of open-source); • **Insufficient demand and lack of market fit:** The proposed solutions may not be competitive with existing systems, especially when part of cost • The usage of secure hardware in Bitcoin-related domains is not yet with clearly established design patterns (distributed backup, multisignature authorization, compatibility, fail-over, heritage…); • **Legal and regulation limitations** for usage and research on privacy-enhancing technologies. Examples being recent cases against Tornado Cash (09/2022), Samourai Whirlpool (04/2024) and resulting stop of Wasabi CoinJoin coordinator (05/2024). Increased attempts to regulate self-custodial wallets.

3.2.5 Post-Quantum Cryptography

General Description

The post-quantum cryptography (PQC) and quantum-safe technologies have received significant attention since the start of the CHESS project (2023). Czech Republic became part of the Euro-QCI initiative, which has the aim to build quantum-safe communication infrastructure across EU. In the Czech Republic, this activity should be realized by the CZ-QCI project, a Digital Europe-financed project run by a consortium of mainly academic partners, including Brno University of Technology and Masaryk University, partners of CHESS. Although CZ-QCI project contains some activities in PQC, most of the activities are focused on QKD (Quantum Key Distribution) technologies.

The Czech National Cyber and Information Security Agency (NUKIB, partner of CHESS) is already very active in the area of quantum-safe technologies. Particularly, it released the *Minimum Requirements for Cryptographic Algorithms*[8], which is a document containing mandatory requirements on algorithms used in critical systems. Recommendations on the post-quantum cryptography transition are part of the document. The topic of quantum and

[8] https://nukib.gov.cz/download/publications_en/Minimum_Requirements_for_Cryptographic_Algorithms_final.pdf

post-quantum security is also identified by the *National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025*[9] as one of the future challenges.

Furthermore, a number of R&D projects besides CHESS are focused on the topic of post-quantum cryptography. These are more engineering-based and focused on practical deployment. The NESPOQ[10] project is an example of such a project, funded by the Ministry of Interior and solved by the Brno University of Technology, CESNET and the Technical University of Ostrava.

In relation to PQC, the Czech National Quantum Strategy is being drafted by Petr Kavalíř, who has been appointed as the Commissioner for Quantum Technologies.

Besides CHESS consortium members, there are activities in other academic teams. Most related work is in the area of PQC implementation analysis, which is addressed by the Czech Technical University, the team of Dr. Martin Novotny.

Estonia is also a member of the Euro-QCI consortium since October 2020. However, the systematic activities concerning post-quantum cryptography started already in 2016, when the topic was first covered in the periodic report on cryptographic algorithms life-cycle[11]. A dedicated report on post-quantum cryptography was released in 2018[12]. As Estonia is one of the leading countries in remote electronic voting, an important part of the post-quantum research is devoted to electronic voting in the post-quantum era. Cryptographic primitives required for such applications were explicitly left out of the focus of the NIST standardization effort, so a separate line of research is needed for it. Accordingly, researchers at Cybernetica have been working on it since 2020. NIST has been the most active and progressive player in this field, and currently, they have three standards in a draft version for which everyone is welcome to submit comments and participate in the discussion without having to go through a long process to establish a liaison relationship. Moreover, these standards, once final, are available free of charge, unlike most standards from ISO/IEC and CEN/CENELEC. The CHESS project (CA 5) has been following and contributing to the work in the NIST PQC project. Currently, NIST PQC has three drafts in progress: FIPS 203 (Draft) Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204 (Draft) Module-Lattice-Based Digital Signature Standard and FIPS 205 (Draft) Stateless Hash-Based Digital Signature Standard.

Key Stakeholders

Multiple CHESS partners are involved in CA5-related activities. The main contributors include:

- Cybernetica: research and development company being responsible for developing many cryptographic e-government solutions for the Estonian government, with several of the solutions also being deployed abroad.

[9] https://nukib.gov.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf
[10] https://www.nespoq.cz
[11] https://www.id.ee/wp-content/uploads/2020/02/cryptographic_algorithms_lifecycle_report_2016.pdf
[12] https://www.id.ee/wp-content/uploads/2022/11/postkvant-kruptograafia-ulevaade-2018.pdf

- Guardtime: Guardtime’s competencies and R&D interests include data security, privacy, cryptography (post-quantum, hash-based), privacy-preserving mechanisms, secure data collaboration via auditable MPC, scalable cryptocurrency systems, and the implementation of blockchain solutions for supply chain challenges.
- Brno University of Technology: academic partner running research, implementation and education in PQC.
- NÚKIB: governmental agency, Czech cybersecurity authority releasing recommendations and policy documents on PQC.
- RedHat: company involved in the implementation aspects of PQC in software systems, mainly open-source.

Besides the CHESS consortium, there are multiple institutions in government, industry and academia dealing with post-quantum cryptography. The most relevant (and those that have some relationship with CHESS partners) are: Proficomms, Magmio, BrnoLogic, IMA, CESNET, Ministry of Interior of Czech Republic, Czech Security Information Service, and others.

However, all companies, not only those mentioned above, can use the results of CA5 – postquantum technologies to make their communication resistant to quantum attacks and to further improve their products.

Cooperation and Best Practices

Currently, CA5 is managed by Cybernetica and Brno University of Technology. Both organisations contribute to common goals, with Cybernetica more focused on technologies used for authentication and integrity assurance and BUT focused more on encryption and Key Encapsulation Mechanisms (KEMs). As of 2024, both partners work jointly on establishing the first Czech-Estonian quantum-safe channel, which will be protected by the means of PQC. For this task, staff often travel to cooperating institutions and joint events are organized, such as brokerage events and summer schools. The team is led by Jan Willemson on the Estonian and Jan Hajny on the Czech side.

Knowledge transfer needs and opportunities

CA5 partners organize common events for the consortium and for public, mostly on post-quantum cryptography-related topics. The events range from awareness-raising to highly technical talks.

Training CA5 needs or would find beneficial, i.e. needs identified by Czech CHESS partners:

- Legal aspects of quantum and post-quantum technologies

Training CA5 can offer to the project partners (and beyond):

- Share recent developments in post-quantum cryptoalgorithms, risk assessment of practical information security products, usability of quantum technologies via cross-border seminars.

- Increase skills for practically evaluating quantum and post-quantum tech via practical hands-on workshops and study exchanges in BUT's Quantum Security lab and Cybernetica.
- Educate the public on the benefits of post-quantum technologies where they will be introduced.
- Help policymakers to plan for the post-quantum transition strategies.

SWOT Analysis

Table 5: SWOT analysis: Post-Quantum Cryptography

Strengths	Weaknesses
• PQC is a hot topic due to quantum threat • No other technology can provide such solutions • PQC is relatively easy for implementation • CHESS consortium already offers some prototypes	• PQC is more demanding on resources • PQC needs some infrastructure updates • Some existing technologies not ready for (PQC) changes (PKI….)
Opportunities	**Threats**
• National authorities already recommend PQC • PQC is in standardisation • PQC is already part of some cybersecurity strategies • There is a lot of market potential	• There may be security weaknesses in PQC • Standardisation process may take longer • Other solutions than PQC (such as QKD) may prevail

3.2.6 Human-Centric Aspects of Cyber-Security

General Description

Human-centric aspects of cybersecurity focus on the interactions between people and technology, emphasizing user behaviour, awareness, and education to enhance security measures. In South Moravia, significant efforts have been made to improve cybersecurity education and awareness through initiatives and collaborations among academia, industry, government, and non-governmental organizations. Estonia, renowned for its advanced digital infrastructure, has implemented comprehensive cybersecurity education programs and public awareness campaigns, positioning it as a leader in integrating human-centric strategies into national cybersecurity policies. Both regions underscore the critical importance of addressing the human element to effectively mitigate cyber risks.

Key Stakeholders

In South Moravia, key cybersecurity stakeholders play vital roles, contribute significantly, and enhance the region's cybersecurity landscape. The National Cyber and Information Security Agency (NÚKIB), based in Brno, coordinates national efforts, sets policies, and responds to cyber threats. Masaryk University and Brno University of Technology contribute through cutting-edge research and specialized training, preparing a skilled workforce. The region's dynamic tech industry, including numerous IT (global) companies and startups, drives innovation and collaborates with academia and government to develop advanced technologies and practices. In Estonia, key cybersecurity stakeholders include the Estonian Information System Authority (RIA), which is responsible for national cybersecurity, coordinating cyber defence, and managing the country's digital infrastructure. Tallinn University of Technology and the University of Tartu, engage in advanced cybersecurity research and offer specialized educational programs. Additionally, technology companies like Cybernetica, Guardtime, Talgen Cybersecurity, Rangeforce, Cybexer Technologies, Clarified Security are developing cybersecurity solutions and collaborating with public institutions on security initiatives.

Cooperation and Best Practices

Collaborating on hands-on cybersecurity training involves a multifaceted approach. We identify skill gaps, develop the training with input from academia, industry, and government, and deliver training through various hands-on events (onsite, remote, hybrid). We perform research and training activities using the KYPO cyber range platform (hands-on exercises) and INJECT exercise platform (tabletop exercises) – state-of-the-art cybersecurity research and education tools. These learning environments enable learning using authentic tools, systems, and methods used in practice. The current best practice is to incorporate realistic scenarios into the training, allowing participants to apply their knowledge practically and better prepare for real-world challenges.

Cooperation with cybersecurity stakeholders in the area of penetration testing report usability actually went even more successfully than expected. Researchers from MUNI organized several workshops in Czechia and Estonia (they are in a tight collaboration with CYBER) reaching out to representatives of many companies outside the CHESS consortium. The events were tailored to cater to a diverse audience, ranging from technical professionals such as developers, validators, and administrators, to cybersecurity managers and decision-makers. A noteworthy discovery from these exercises is that focus groups organized after the workshops with collection of survey responses bring extremely valuable insights that otherwise may not be observed from the surveys only.

Knowledge transfer needs and opportunities

Knowledge transfer between South Moravia and Estonia presents significant opportunities for collaboration and mutual growth in cybersecurity, especially in training and capacity building. South Moravia can leverage Estonia's expertise in hands-on cybersecurity training (e.g., a huge ecosystem of companies dedicated to cyber training) and certification programs to enhance its own workforce's skills and capabilities. Similarly, Estonia can benefit from South Moravia's innovative approaches to cybersecurity education and awareness initiatives.

Workshops in the area of penetration testing report usability call for instructors who have both some technical knowledge about penetration testing and also are well-versed in interactions with people who follow other interests than just the expected workshop participation lessons/insights. Our workshops showed that training for such instructors can be well provided when a workshop is instructed by a couple of instructors – at least one with technical knowledge and another with people skills.

Training CA6 need would find beneficial:

We are seeking a comprehensive training program covering technology transfer, intellectual property (IP) development, research management, and writing project proposals for academic and research professionals. Key areas include understanding technology transfer, mastering IP concepts, optimizing research management, and crafting compelling project proposals. Objectives include providing practical insights, enhancing IP proficiency, improving research impact, and developing strong proposal writing skills. The target audience comprises faculty, researchers, and doctoral students. Flexible formats, such as workshops or online modules, are preferred. We aim to equip participants with practical skills to excel in these areas. Additionally, we need to attract, hire, and retain highly skilled and motivated students by offering advanced research, training, and development opportunities, creating a supportive environment that encourages their continuous learning and professional growth.

For usable security – and well beyond the area of penetration testing report usability – we need to train more people (namely graduate students) in surveying, running workshops and also facilitating focus groups to gather the experience and insights of the subjects.

Training CA6 can offer to the project partners (and beyond):

We are innovating the current practice of tabletop exercises by researching and developing new methods and software tools to enhance skills in both technical and non-technical fields of cybersecurity. Tabletops are highly effective for delivering cybersecurity training because they provide interactive, real-world scenarios that enhance understanding and retention of cybersecurity concepts. These exercises promote collaboration and communication, essential for incident response while helping participants develop quick decision-making skills under pressure. Tabletops also allow organizations to identify and address gaps in their cybersecurity policies and procedures cost-effectively.

We are also organising workshops on work with penetration testing reports, providing valuable insight into the process of penetration testing for both people involved in the technical aspects and for individuals overseeing cybersecurity strategies. We show the participants what is happening before receiving a penetration testing report and we create opportunities for cybersecurity professionals from different sectors to meet and share experience with penetration testing.

SWOT Analysis

Table 6: SWOT Analysis: Human-Centric Aspects of Cyber-Security

Strengths	Weaknesses
• **Collaborative Expertise:** South Moravia (SM) and Estonia (EE) bring together **diverse cybersecurity expertise**, with EE being a global leader in digital security and SM having strong educational institutions. • **Continuous Improvement:** Human-centric approaches emphasize continuous	• **Resource Allocation:** Coordinating resources and **priorities** between **various stakeholders** and **regions** can be challenging, leading to **inefficiencies**. • **Participant Engagement:** The **effectiveness** of trainings **depends** on the active **participation** and **engagement** of all involved, which can vary.

improvement, helping stakeholders **stay ahead** of evolving **cyber threats**. • **Interactive Learning:** Tabletops provide **hands-on**, interactive **training** that **enhances understanding** and retention of cybersecurity concepts. • **Cost-Effective:** Compared to full-scale exercises, **tabletops** are relatively **low-cost** and simpler to organize, requiring **fewer resources**. •	• **Cybersecurity Disparities:** Variations in cybersecurity **maturity levels** and **expectations** between the stakeholders, organizations, and regions is challenging.
Opportunities	**Threats**
• **Joint Training Programs:** Develop **cybersecurity training programs** that incorporate the strengths of both regions, focusing on **education** and **practical skills**. • **Research and Development:** Encourage further **joint R&D projects** to innovate new cybersecurity solutions, **leveraging** the strengths of **both regions**. • **Customized Training:** Tabletops can be tailored to **address specific** organizational **needs**, **threats**, and **regulatory requirements**, enhancing impact.	• **Evolving Threat Landscape:** Rapid changes in cyber threats **require constant updates** to **training scenarios** to **remain relevant** and effective. • **Resource Competition: Competition** for cybersecurity **talent** and **funding** limits the **effectiveness** of proposed **initiatives**. • **Project based research**: a lot of risk for someone who wants to focus on a new topic. There is a **need** for more **long-term** general **research grants**. • **Geopolitical Risks:** Regional **geopolitical tensions** could impact the **stability** and **continuity** of **collaborative** cybersecurity efforts.

4 Conclusions

In this final chapter, we draw together the insights and findings from our extensive analysis of the cybersecurity research and innovation (R&I) landscape in South Moravia and Estonia. Throughout the CHESS project, we have embarked on a comprehensive journey, exploring various facets of the cybersecurity domain, from the regulatory frameworks to the dynamic interactions among key stakeholders in both regions. Our SWOT analysis has provided a structured evaluation of strengths, weaknesses, opportunities, and threats, revealing critical paths for future initiatives.

The conclusions presented herein synthesize the best practices identified during the project, propose key recommendations for advancing the cybersecurity agenda, and outline strategic next steps to ensure sustainable growth and resilience in the face of evolving digital threats. By consolidating these elements, this chapter aims to provide a clear roadmap for stakeholders involved in the CHESS project and serve as a guideline for policymakers, industry leaders, and academic entities as they continue to enhance the cybersecurity infrastructure and capabilities within and beyond the regions of South Moravia and Estonia.

Let us now reflect on the foundational accomplishments and look forward to the strategic initiatives that will drive the future of cybersecurity research and innovation in these vibrant technological ecosystems.

4.1 Best practices

Through its thorough analysis and collaborative efforts in South Moravia and Estonia, the CHESS project has identified several best practices across different challenge areas in cybersecurity. These practices not only enhance the effectiveness of current security measures but also set a precedent for future initiatives in the region and beyond. Here, we outline these practices, illustrating their application and impact within the cybersecurity domain.

- **Interdisciplinary Collaboration**: A recurring theme across all challenge areas is the vital importance of interdisciplinary collaboration. Bringing together experts from academia, industry, and government has led to more comprehensive approaches to tackling cybersecurity challenges. This synergy facilitates a deeper understanding of threats and more innovative solutions. For instance, in the area of the Internet of Secure Things (IoST), collaboration between technical experts and regulatory bodies has helped in developing standards that ensure device security without stifling innovation.
- **Continuous Knowledge Transfer**: Continuous education and training programs are essential for keeping the workforce updated with the latest security practices and technologies. The project has highlighted successful models of ongoing professional development, such as workshops, certified courses, and webinars that focus on emerging threats and new technologies like blockchain and quantum cryptography. These initiatives help maintain a high level of readiness against potential cyber threats.

- **Public-Private Partnerships (PPPs)**: Effective PPPs have been crucial in pooling resources and expertise to address cybersecurity challenges more efficiently. These partnerships have not only accelerated the development of technological solutions but have also ensured that these solutions are pragmatic and tailored to real-world needs. For example, the collaboration between universities and tech companies in developing and testing new encryption algorithms has led to innovations that are both academically sound and industrially viable.
- **Adaptive Regulatory Frameworks**: In the dynamic field of cybersecurity, static regulatory frameworks can quickly become obsolete. Best practices identified in the project include the development of adaptive regulatory mechanisms that can evolve in response to new challenges and technologies. This approach has been particularly effective in Estonia, where digital governance frameworks are periodically reviewed and updated to incorporate new security protocols and address emerging digital risks.
- **Community Engagement and Awareness Programs**: Raising awareness about cybersecurity issues is a fundamental best practice that empowers individuals and organizations to protect themselves against cyber threats. Successful community engagement strategies have included national cybersecurity awareness campaigns, public seminars, and the integration of cybersecurity education in schools. These efforts demystify cybersecurity and promote safer online behaviours across all segments of society.
- **Leveraging Advanced Technologies**: Utilizing cutting-edge technologies such as AI and machine learning for defensive and offensive cybersecurity operations has set a best practice standard in both predictive threat analysis and incident response. These technologies have enabled more sophisticated monitoring of network activities and quicker responses to security breaches, significantly enhancing the overall security posture.

By institutionalizing these best practices, the CHESS project aims to create a robust cybersecurity ecosystem that is capable of not only responding to current threats but also anticipating and mitigating future risks. As we move forward, these practices will form the cornerstone of a resilient digital environment in South Moravia, Estonia, and potentially across Europe.

4.2 Key recommendations

As we navigate the complex landscape of cybersecurity research and innovation (R&I) in South Moravia and Estonia, the CHESS project has delineated several key recommendations across different challenge areas. These recommendations are designed to guide stakeholders towards a more secure, resilient, and innovative cybersecurity ecosystem. Herein, we detail these recommendations, categorized by their respective challenge areas, to facilitate targeted and effective enhancements in cybersecurity practices and policies.

Internet of Secure Things (IoST):

- Enhance Device Security: Develop and enforce enhanced security standards and regulations for IoST devices to prevent breaches and attacks. This includes mandatory security audits and the integration of security by design principles.

- Promote Interoperability: Encourage the development of interoperable security protocols to ensure seamless and secure communication between diverse IoST devices and systems.
- Increase User Privacy: Develop and apply methods that protect user privacy by secure data handling and by advanced authentication methods. Deploying Privacy-enhancing technologies into user-based IoST use cases.
- Focus on Emerging IoST Use Cases: Design and develop advance security protocols for emerging use cases such as smart transportation, autonomous automotive, etc.

Security Certification:

- Standardize Certification Processes: Establish a unified and standardized certification process for cybersecurity products and services to build trust and facilitate market acceptance. Increase transparency of the security certification process. Help build certification institutional backing (accredited conformity assessment bodies and labs).
- Increase Accessibility: Make cybersecurity certifications more accessible to small and medium-sized enterprises (SMEs) by subsidizing the cost and simplifying the certification procedures.
- Provide Tools: Equip stakeholders (SMEs, public organisations, etc.) with tools that can be used to verify their cybersecurity posture and level of compliance with security standards and requirements.

Verification of Trustworthy Software:

- Invest in Automated Tools: Support the development of advanced automated verification tools that can efficiently handle the increasing complexity and volume of software.
- Invest in Tool Prototyping and Deployment: Hundreds of verification tools or methods exist and are nourished in the academia yet are often tested in only university laboratories and by the researchers themselves. Deployment and piloting in the computer industry must be supported, and the tools must be tested in real life, in actual development cases and in their quality assurance processes.
- Promote Open Standards: Advocate for the adoption of open standards in software verification to enhance transparency and collaboration in the development of secure software.

Security Preservation in Blockchain:

- Focus on scalable solutions: Encourage research into scalable security solutions that can support the growing use of blockchain technologies across various sectors. Promote the integration of blockchain in various application domains such as healthcare, intelligent transportation and infrastructure to enhance security and transparency in a multistakeholder environment.
- Enhance awareness regarding blockchain-based applications’ security: Establish a unified framework and knowledge base that can explain the security threats that appear in blockchain-based applications and how to mitigate them.
- Educate the industry and the general public on the merits of a given blockchain-related technological idea. The entities in the space frequently overplay the importance of one specific idea and even use primarily novelty instead of merit to drive short-term interest into a specific blockchain solution ("pump-and-dump" schemes, use blockchain

"everywhere"). A robust understanding of the problem solved and trade-offs made is desirable.

- Increase end-user understanding of the importance and available techniques of secure private keys handling and backup: As digital identity and digital assets control increasingly moves from centralized services to end users, thus increasing privacy and robustness, more responsibility is also moved to end-users.

Post-Quantum Cryptography:

- Accelerate Research and Development: Prioritize and fund research into post-quantum cryptographic algorithms to prepare for the quantum computing era.
- Foster Public-Private Partnerships: Leverage partnerships between government, academia, and industry to share knowledge and resources in the development of quantum-resistant cryptographic solutions. Participate in the development of standards and contribute to their improvement.
- Raise Awareness about Quantum-Related Threats: organize workshops, seminars, conferences and other events to inform the public about the process of post-quantum cryptography transition.
- Show Good Practices and Create Demonstrators for Post-Quantum Transition: deliver examples and prototypes of technologies resilient to quantum threats.
- Produce and Participate in Strategic Roadmaps: comment, review and manage (national) recommendations and roadmapping documents related to quantum-safe technologies.
- Support Training and Education in Post-Quantum Cryptography: propose, design and implement novel courses, modules and programs on quantum-safe technologies.
- Support Piloting Activities: design, deploy and support practical pilots for post-quantum technologies, with real-world applications and verification in multiple sectors of the quadruple helix. Collect feedback from a wide spectrum of end-user representatives.

Human-Centric Aspects of Cyber-Security:

- Enhance Cybersecurity Training: Implement comprehensive training programs focusing on the human elements of cybersecurity to reduce the risk of human error and increase overall security awareness.
- Promote the Concept of Mental Models (mental model is a user’s view – correct or otherwise – of how a system works and the consequences of user actions) in design and implementation of security solutions. And enforce the “you are not your user” principle in developing these security solutions.
- Train Cybersecurity Experts – to understand the concepts of usable security and assist them in implementing these concepts in their activities.
- Integrate Behavioural Studies: Include behavioural studies in cybersecurity strategy planning to better understand and mitigate risks associated with human behaviour.

To support the implementation of these recommendations, strong cross-sectoral and international cooperation would be essential. By fostering collaborations across different sectors—government, academia, industry, and non-governmental organizations—a rich ecosystem of knowledge, resources, and best practices can be developed. Such partnerships facilitate the integration of diverse perspectives and expertise, which is critical for addressing complex cybersecurity challenges. For instance, collaborative efforts can lead to the development of robust security protocols for the Internet of Secure Things (IoST) that are universally applicable and adaptable across different industries and countries. Furthermore, these partnerships can enhance the efficacy of security certifications by ensuring that they are recognized internationally, thus reducing redundancy and promoting a global standard in cybersecurity measures.

Moreover, cross-sectoral and international collaborations can significantly contribute to advancements in areas like post-quantum cryptography and blockchain security. By pooling resources and knowledge from around the world, researchers and practitioners can accelerate the development of quantum-resistant cryptographic methods, ensuring that these new technologies are secure against future threats posed by quantum computing. In the realm of blockchain, shared efforts can lead to the establishment of universal security standards that address the unique challenges posed by decentralized technologies, while also fostering innovation and trust in blockchain applications globally. These collaborative frameworks not only help in aligning cybersecurity strategies across borders but also in ensuring that the protective measures are inclusive, cutting-edge, and effective against a broad spectrum of cyber threats. Such a holistic approach is essential for creating a resilient digital infrastructure that can withstand the complexities of modern cyber environments.

By implementing these recommendations, stakeholders in South Moravia, Estonia, and beyond can enhance their cybersecurity frameworks, protect against emerging threats, and foster an environment conducive to technological innovation and security. These actions will not only address immediate vulnerabilities but also pave the way for future advancements in cybersecurity resilience.

4.3. Next steps

Building upon the outcomes of the SWOT analyses conducted across various challenge areas in the CHESS project, it is essential to formulate a strategic action plan that guides the project consortia toward achieving enhanced cybersecurity research and innovation in South Moravia and Estonia. This document is the first step towards achieving three of the main objectives of the CHESS project:

- Creating the cross-border joint cybersecurity R&I strategy aligned with CZ-EE smart specialisation strategies (ICT) and Europe's digital society and cybersecurity goals as articulated in the roadmaps developed by four H2020 Cybersecurity flagship projects. These are Cyber Security Competence for Research and Innovation (CONCORDIA), Strategic programs for advanced research and technology in Europe (SPARTA), Cyber Security for Europe (CyberSec4Europe) and the European Network of Cybersecurity Centers and Competence Hub for Innovation and Operations (ECHO);
- Action and investment plans for implementation of the strategy in each of its six focus areas of cybersecurity;
- Training strategy for both regions to increase cross-border/sectoral cooperation and increase needed skills around the six priority areas.

The CHESS action plan will focus on leveraging strengths, addressing weaknesses, capitalizing on opportunities, and mitigating threats identified during the analyses.

- **Strengthening Research and Development Capacities:**

  - Enhance Infrastructure: Invest in upgrading and expanding the technological and research infrastructure to support advanced cybersecurity studies and innovations, particularly in emerging areas like post-quantum cryptography and Internet of Secure Things (IoST).
  - Foster Academic and Industrial Partnerships: Develop formal partnerships between academic institutions and industry leaders to facilitate the practical application of research findings and to bring academic innovations to market more swiftly. Utilize CHESS brokerage events and bodies like the Advisory Group and the Exploitation Board for this purpose – and oversee this in a dedicated session of the CHESS Strategy Board.
- **Expanding Educational and Training Programs:**
  - Curriculum Development: Implement specialized cybersecurity curricula that address current and emerging security technologies and challenges, ensuring that educational offerings remain relevant to the needs of both the public and private sectors. Existing skills frameworks like ECSF[13] or Czech CyQUAL[14] and related tools may be implemented.
  - Continuous Professional Development: Establish ongoing training programs for professionals to keep pace with the rapid developments in cybersecurity, emphasizing hands-on training and certifications that are recognized across sectors and borders. Professional training programs should also be built on existing frameworks and could be supplemented by certification mechanisms such as the one developed by REWIRE project[15] or by the implementation of microcredentials mechanisms that are being developed in Czechia[16].
- **Enhancing Cross-Sectoral and International Cooperation:**
  - Establish Collaborative Networks: Create networks that connect different stakeholders—government agencies, educational institutions, private sector entities, and international organizations—to facilitate the sharing of resources, knowledge, and best practices.
  - Participate in International Initiatives: Actively engage in international cybersecurity initiatives and frameworks to ensure alignment with global standards and to influence international policy development.
- **Promoting Innovation and Commercialization:**
  - Support Startups and SMEs: Provide targeted support for startups and small and medium-sized enterprises (SMEs) working on cybersecurity innovations through grants, mentorship, and access to testing environments.
  - Incentivize R&D in Key Areas: Promote implementation of incentives like funding grants to encourage research and development in specific high-impact areas such as blockchain security and AI in cybersecurity.
  - Promote deployment and commercialisation thanks to the support of the regional innovation ecosystem. We will engage ecosystem interfaces (RIA, CSH, NCISA and JIC) in the provision of a comprehensive support system to innovators, spin-offs, and emerging entrepreneurs. Regional start-up competitions, incubation spaces, business consultancy services, and

[13] European Cybersecurity Skills Framework – see online: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

[14] Czech National Cybersecurity Qualifications Framework – see online: https://www.cyqual.cz.

[15] For more see: https://rewireproject.eu/certification/.

[16] For more see: https://www.npi.cz/aktuality/7778-mikrocertifikaty-system-rozvoj-jednotlivce.

entrepreneurship training will be promoted to the CHESS community and the broader cybersecurity R&I ecosystem in South Moravia and Estonia. CHESS will organize:

a. Technology transfer days, i.e. cross-border knowledge exchange primarily between academic and industrial organizations. Four events in total, with one Industrial Day already successfully organized at the end of 2023.
b. Brokerage events will be organized to bring together relevant stakeholders from both regions across the quadruple helix, with an emphasis on researchers and IT professionals. Participants will be engaged in networking exercises and be invited to work on the challenge areas together. Six events are planned in total, the first two planned (one in each region) for 2024.

- **Implementing Regular Updates:**
  - Regular SWOT Updates: Conduct regular SWOT analyses to continuously assess the changing landscape of cybersecurity threats and opportunities, ensuring that the consortia can adapt and respond effectively.
  - Monitoring the progress within each Challenge Area. Each of the six teams working on a Challenge Area will set specific sets of KPIs to track the progress. This will be included in *D1.2 Strategy for Cross-Regional Collaboration in Cybersecurity,* due in December 2024.
- **Advocating for Supportive Policy Frameworks:**
  - Policy Advocacy: Engage with policymakers to advocate for laws and regulations that support cybersecurity innovation, protect privacy, and foster international cooperation.
  - Public Awareness Campaigns: Initiate public awareness campaigns to educate citizens and businesses about cybersecurity risks and best practices, thereby enhancing the overall security culture.

By following this structured action plan, the CHESS project consortia can effectively move forward, leveraging the strengths identified in the SWOT analyses to address the weaknesses and threats, while also capitalizing on the abundant opportunities for advancing cybersecurity capabilities in South Moravia and Estonia. This proactive approach will not only bolster the regions' cybersecurity resilience but also position them as leaders in the global cybersecurity landscape.

Annex 1: Questionnaire

Annex 1 includes the questionnaire prepared for the purpose of gathering information about the state of play across all Challenge Areas in both regions.

Regional academic expertise:

1. Academic/research institutions/teams in the region you cooperate with in the area of cybersecurity and how they are relevant to the Challenge Area you are involved in.
2. Are there any academic institutions/teams in the region you do not currently cooperate with but might be interesting for you/CAs you are involved in? If so, please specify.

Regional industry expertise:

3. Companies in the region you cooperate with in the area of cybersecurity.
4. Companies in the region you do not currently cooperate with but might be interesting for you/CAs you are involved in.
5. Which of the companies listed above can use the research results from your area, and how? Can your results be deployed to some of them?

Other regional players:

6. What are any other major regional players active in your area you know about?

   Examples:
   - Relevant public authorities, e.g., NÚKIB, UOOÚ (The Office for Personal Data Protection).
   - Relevant NGO/non-profits (e.g., CyberHub, Czechitas)
   - Funding, start-up ecosystem (JIC, Digital Innovation Hubs, etc.)
   - Relevant education/training providers (schools, providers of courses/training, etc.)

7. Do you cooperate with any of them? How? Which of them can use the results of research from your area, and how? Can your results be deployed to some of them?

European context:

8. Do you know of any relevant networks, organisations, institutions, governmental institutions (national/EU), or EC Agencies that might be relevant to your activities (activities within your Challenge Area)? Do you already cooperate with some of them?
9. Do you know of any national or EU/international projects (past or ongoing) relevant to your research that you think have the potential to move your field forward?
10. Is there some major national/regional policy/strategy/regulation for the area (legislation, standards, blueprints, strategies developed by a public institution or standardisation body at the national level)?

11. Is there some major European policy/strategy/regulation for the area (legislation, standards, blueprints, strategies developed by a public institution or standardisation body at the EU level)?

Global position:

12. Who are the world leaders in your area (both in research and industry)? Do you cooperate with any of them? If so, how?
13. What are the global trends in your area (feel free to provide any relevant information, such as main challenges, recent developments, new technologies/solutions, etc.)?
14. Is there anyone from abroad you would like to establish new cooperation with? What could help to start the cooperation?

Needs, Opportunities, Training:

15. What would help you move your crucial research activities forward? Please feel free to provide any relevant information – financial support, access to infrastructure, new cooperation, changes in legislation, etc.
16. Is there any infrastructure in your institution or region that you are missing? If so, please specify.
17. What Instruments/tools to promote cross-sectoral cooperation do you have experience with? What do you miss?
18. Is there any training you or your team would find helpful? If so, please specify. (e.g., research training, entrepreneurship training, transferable skills, e.g., proposal writing, public speaking)

Cross-regional cooperation

19. For Czechs: Are there any institutions/teams in Estonia that are not part of CHESS but you cooperate with or would like to cooperate with? If so, please specify.
20. For Estonians: Are there any institutions/teams in the Czech Republic that are not part of CHESS but you cooperate with or you would like to cooperate with? If so, please specify.

Other

21. How do you finance your activities? What are other possible sources of funding?
22. Is there any support from your institution/regional/national bodies that you miss? If so, please specify.
23. What makes your institution potentially attractive for international students or employees? What are the barriers (what could help make your institution more attractive for international students/employees?)