D1.4 Roadmap for Cross-Regional Collaboration in Cybersecurity

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	D1.4
Deliverable name	Roadmap for Cross-Regional Collaboration in Cybersecurity
Lead Beneficiary	RIA
Type	R – Document, report
Dissemination Level	PU – Public
Work Package No	WP1
Date	30 June 2026
Version	1

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)

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)
- Triin Muulmann (TalTech)

Reviewers

- Lauri Tankler (RIA)
- Airi Aljas (RIA)
- Václav Matyáš (MUNI)
- Zuzana Vémolová (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 Association of Information Technology and Telecommunications (associated)	ITL	Estonia

Abbreviations

AI/ML – Artificial Intelligence / Machine Learning
CC – Common Criteria
F4SLE – Framework for Security Level Evaluation
IoST – Internet of Secure Things
IoT – Internet of Things
MASS – Maturity Assessment System
MPC – Multi-Party Computation
NGO – Non-Governmental Organisation
NIS2 – Network and Information Security Directive (EU)
NÚKIB – National Cyber and Information Security Agency
PQC – Post-Quantum Cryptography
PP – Protection Profile
R&I – Research and Innovation
ST – Security Target
VPN – Virtual Private Network
WP – Work Package

Executive Summary

This roadmap constitutes the final strategic deliverable of the CHESS project. It builds on the foundational SWOT analyses (D1.1[1]) , cross-regional strategies (D1.2[2]) , and action plans (D1.3[3]) developed and implemented within *Work Package 1 Strategy Development and Sustainability of the Hub*. The document summarises the experience gained in CHESS and outlines how cooperation between Estonia and South Moravia will continue beyond the project lifetime.

The roadmap is structured around a set of cross-cutting actions that define how collaboration, research and innovation activities, mobility, ecosystem engagement and policy interaction will be sustained across all Challenge Areas. These actions provide a shared framework for continuation.

This cross-cutting perspective is complemented by dedicated roadmaps for each of six Challenge Areas, which capture the thematic continuation of research and innovation activities, as well as domain-specific collaboration. Together, these two levels offer a comprehensive view of how CHESS collaboration will continue, combining a common strategic approach with detailed implementation pathways in specific domains.

While CHESS itself is a time-limited initiative, it has created a strong and well-connected collaboration network. The hub will remain active through follow-up projects, ongoing cooperation and lightweight coordination tools. The roadmap presents a set of practical actions to support the continued development, dissemination and uptake of CHESS results, offering a realistic and implementation-oriented model for sustaining CHESS results.

[1] Deliverable D1.1 Training and knowledge transfer needs and opportunities (SWOT) in South Moravia and Estonia
[2] Deliverable D1.2 Strategy for Cross-Regional Collaboration in Cybersecurity
[3] Deliverable D1.3 Action Plans for 6 CHESS Challenge Research Areas

Table of Contents

1 Introduction

The Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) brings together leading cybersecurity institutions from both regions to address important cybersecurity challenges. The project connects universities, companies of different sizes, public information-security bodies, and community actors, covering all four sectors of the quadruple helix: research, industry, public sector, and civil society. By integrating research, innovation, and practical applications, CHESS aims to strengthen regional and European cybersecurity resilience.

Over the course of the project, CHESS has evolved from an initial coordination and ecosystem-building effort into a collaborative platform delivering concrete research and innovation outputs, pilot activities, training initiatives, and cross-sectoral knowledge exchange. These activities have demonstrated the value of targeted, cross-regional collaboration in advancing cybersecurity capabilities while building lasting institutional relationships between Estonia and South Moravia.

As the project reaches its conclusion, the focus shifts from implementation to continuity. The purpose of this roadmap is to consolidate the experience gained within CHESS and to define how its results, partnerships, and collaboration mechanisms will be sustained and further developed beyond the project lifetime. Rather than establishing new formal structures, the continuation model builds on existing networks, follow-up projects, and lightweight coordination mechanisms that enable flexible and demand-driven cooperation.

This roadmap therefore outlines the current state of CHESS outcomes, identifies the most promising areas for continuation, and defines a set of priority actions to support ongoing collaboration, further development of results, and their uptake in practice. It reflects a realistic approach to sustainability, highlighting both secured continuation pathways and areas where further effort, resources, or coordination are needed.

2 Key Stakeholders and Roles

The CHESS project brings together universities, companies of different sizes, public information-security bodies, and community actors, thereby covering all four sectors of the quadruple helix: research, industry, public sector, and civil society. The roadmap defines how this multi-sector collaboration is sustained and further developed by addressing the needs and roles of the key stakeholder groups, as well as the enabling actors that support the long-term evolution of the hub.

The roadmap first addresses the CHESS Consortium, which acts as the core enabling structure for continuity and sustainability. The nine beneficiaries and three associated partners provide strategic leadership and institutional anchoring of the CHESS hub within regional and national ecosystems. Their continued cooperation ensures that technical results and collaborative practices developed within the project remain active beyond the funded period.

Within the academic sector, the roadmap targets universities, research institutes, and individual researchers and educators already involved in CHESS and related follow-up projects. It also explicitly addresses researchers outside the consortium who are interested in the CHESS thematic areas and may become future collaborators. For academia, the roadmap supports long-term research collaboration, skills development, and the joint development of new research and innovation projects.

The industry sector includes companies of different sizes, ranging from SMEs and startups to larger enterprises, industry associations, and technology providers. The roadmap is particularly relevant for decision-makers and technical leaders such as Heads of R&D, Chief Information Security Officers, Chief Technology Officers, and security architects. It also addresses organisations working with secure digital transactions, identity and wallet solutions, and investors interested in scalable cybersecurity technologies. The roadmap aims to support technology uptake, piloting, and commercial exploitation of CHESS outputs while strengthening industry–academia collaboration.

For the public sector, including governments and policy-makers, the roadmap ensures that research and innovation activities remain aligned with national cybersecurity strategies and evolving regulatory frameworks, such as NIS2 and the Cyber Resilience Act. Target groups include government professionals working in cybersecurity as well as their commercial partners, such as IT solution providers delivering services to the Estonian public sector. The roadmap supports evidence-based policymaking, secure digital infrastructure, and informed adoption of research-driven solutions.

The roadmap also explicitly addresses civil society, understood as actors working in areas such as data protection, digital rights, education, awareness-raising, and community coordination. This includes non-profit organisations and NGOs, volunteer-driven technology communities, and educators, including secondary schoolteachers. Civil-society actors play a critical role as intermediaries and knowledge multipliers, ensuring that cybersecurity expertise, tools, and best practices reach broader audiences and are applied in socially responsible and user-centred ways.

Beyond individual helix actors, the roadmap engages regional ecosystems as a cross-cutting dimension. These ecosystems provide pathways for external institutions from all sectors to access validated CHESS tools and results, such as sec-certs or forensic and assurance frameworks. By embedding CHESS outputs into regional innovation structures, the roadmap supports diffusion, reuse, and long-term impact.

Finally, the roadmap addresses funders as key enabling stakeholders. By providing clear evidence of technical maturity, institutional commitment, and cross-sectoral impact, the roadmap supports future funding from programmes such as Horizon Europe and the Digital Europe Programme. This focus on sustainability ensures that the evolution of the CHESS hub is grounded in verified technical excellence as well as stable organisational foundations. Together, these stakeholder perspectives ensure that the CHESS roadmap supports a coherent transition from a project-based collaboration to a sustainable, multi-sector cybersecurity competence hub embedded within European research, innovation, policy, and societal ecosystems.

3 Methodology and Evidence Base

The CHESS roadmap represents the final consolidation of the strategic work carried out within *WP1 Strategy Development and Sustainability of the Hub*. It builds directly on the preceding deliverables D1.1, D1.2 and D1.3.

D1.1 provided the initial evidence base by mapping training and knowledge-transfer needs and opportunities in South Moravia and Estonia. D1.2 established the strategic framework for cross-regional collaboration in cybersecurity and defined the six Challenge Area strategies. D1.3 translated this strategy into concrete cross-cutting and Challenge Area-specific actions for the final project phase and the period 2026–2029. This roadmap consolidates them from the perspective of the end of the project. It focuses on what has been implemented, what has matured into a sustainable output or cooperation mechanism, what will continue through secured follow-up projects, and where further support, funding or ownership decisions are still required.

The methodology combines document review, partner input collection, Challenge Area leader updates, review of project outputs, and assessment of follow-up projects and proposals. The resulting roadmap is evidence-based, but also practical: it prioritises activities that have a realistic continuation pathway and identifies risks where continuity depends on further funding or institutional commitment.

Review of previous project deliverables

The first step was a review of the previous WP1 deliverables to ensure continuity of logic and terminology across the strategic lifecycle of CHESS.
The review of D1.2 focused on the strategic priorities of the six Challenge Areas, the cross-regional collaboration rationale, the role of the quadruple helix model, and the emphasis on realistic and actionable synergies between Estonia and South Moravia. Particular attention was paid to the strategic aims that cut across all Challenge Areas: strengthening research and innovation cooperation, involving industry and public-sector stakeholders, supporting education and capacity building, and bridging research results with practical adoption.

The review of D1.3 focused on the action plans prepared by the consortium for the final year of CHESS and for the post-project period. This included the cross-cutting actions on broader ecosystem involvement, dissemination events, joint proposal preparation, staff exchange, cooperation with associated partners, and communication and exploitation activities. It also included the CA-specific action plans describing planned R&I activities, events, conference participation, fellowships, policy engagement and outreach.

This review made it possible to distinguish between three categories of content: actions that have already been implemented or are close to completion, actions that remain relevant and should continue after CHESS, and actions that require revision because their continuation depends on new funding, partner capacity or external decisions.

Partner and challenge area input collection

A central part of the roadmap preparation was collecting updated input from the Challenge Area leaders, co-leaders and involved partners. The CA teams were asked to update the information from D1.3 and reflect on the actual implementation status at the end of the project. The requested input covered in particular:

- the status of each mini-project, including whether it is completed, ongoing, continuing after CHESS or discontinued;
- the main outputs produced, such as tools, software, pilots, demonstrators, methods, reports, publications, events or training materials;
- the maturity and usability of these outputs, including whether they are ready for adoption, further piloting, further research or dissemination;
- the concrete cross-regional collaboration evidence, including which partners from Estonia and South Moravia worked together and what results this cooperation produced;
- planned continuation activities after CHESS, including follow-up projects, submitted proposals, national funding, institutional resources or informal cooperation;
- relevant cross-CA dependencies and synergies;
- likely adopters, users or beneficiaries of the outputs;
- main risks, missing resources and support needs.

This input was used to prepare the Challenge Area roadmaps and to identify cross-cutting continuation mechanisms that are relevant for the CHESS hub as a whole.

Review of project outputs

The roadmap also reviewed implementation evidence generated during the CHESS project. This included information on research and innovation activities, mini-projects, demonstrators, tools, training, mobility, dissemination, ecosystem engagement, and policy interaction.

The review focused on the following categories of outputs:

- Mini-projects and research results: The roadmap assessed the status of the 25 initiated mini-projects, distinguishing between completed, ongoing and continuing activities. The objective was not to repeat all technical details, but to identify which mini-projects produced results that can support continued cross-regional collaboration.
- Tools, pilots, methods and demonstrators: Particular attention was paid to outputs with potential for further adoption, piloting or exploitation. These include, for example, tools and methods related to security certification, post-quantum cryptography, blockchain-based security, IoT/IoST security, software verification, training infrastructure and tabletop exercises.
- Training and mobility activities: The roadmap considered workshops, seminars, “train-the-trainer" activities, staff exchanges and fellowships as evidence of capacity building and knowledge transfer. The review assessed which formats were effective

and which can realistically continue after CHESS, especially through SECURE-NET and other mobility or training mechanisms.

- Community and dissemination results: Dissemination activities were reviewed with a focus on mechanisms that helped connect CHESS to wider cybersecurity communities. These include brokerage events, Demo Days, Future Cryptography Conference, RIA CyberMeetUps, SP2I and ETACS workshops, final dissemination events and cooperation with established regional or European platforms.
- Policy and ecosystem engagement: The roadmap reviewed interactions with public authorities, associated partners and ecosystem organisations. This included cooperation with RIA, NÚKIB, JIC, ITL and other relevant stakeholders, as well as contributions to discussions on certification, post-quantum transition, public-sector cybersecurity planning and regional innovation ecosystems

Across all categories, the review considered not only whether an output had been produced, but also whether it had a realistic continuation path, an owner, an expected user group, and a potential source of funding or institutional support.

Review of the follow-up projects and proposals

Follow-up projects and proposals were treated as a key evidence source for sustainability. The roadmap therefore reviewed both secured continuation vehicles and submitted or planned funding opportunities. Three funded follow-up projects are particularly important for the post-CHESS roadmap:

SECURE-NET, which supports continued cross-sectoral collaboration, mobility, knowledge transfer and talent development between CHESS regions and beyond.

CCAT, which provides a continuation pathway for work related to cybersecurity certification and assessment tools.

QARC, which continues and expands work on post-quantum cryptography and practical transition to quantum-resistant solutions;
More information about these projects is to be found below in *Section 4.5 Joint proposals and follow-up projects.*

In addition to these secured projects, the roadmap also considered submitted proposals and planned applications to European, national and regional funding schemes. These proposals are relevant because they show the consortium's continued commitment and strategic direction. However, the roadmap distinguishes clearly between secured funding, submitted proposals, planned initiatives and activities that remain unfunded or only partly funded.

This distinction is important for presenting a realistic sustainability picture. Activities supported by secured projects can be described as confirmed continuation pathways, while activities dependent on submitted or future proposals should be described as conditional or planned.

Assessment of sustainability, ownership and risk

The roadmap applies a sustainability-oriented assessment to the collected evidence. For each major activity or output, the following questions were considered:

- Is there a clear owner or lead partner?
- Which partners are involved in the continuation?
- Is there a secured continuation vehicle, such as CCAT, QARC or SECURE-NET?
- Is the activity supported by national, regional or institutional funding?
- Is the funding secured, submitted, planned, partly secured or missing?
- Does the output have an expected user group or adopter?
- Is further technical development, validation, piloting or dissemination needed?
- What risks may prevent continuation or uptake?
- What resources or decisions are still needed?

This assessment helped identify the main sustainability dependencies across CHESS. These include funding gaps, partial continuation of selected activities, the need for tool maintenance and hosting, dependency on individual researchers or institutional capacity, industry uptake challenges, regulatory and standardisation barriers, and the need to maintain visibility after the project ends.

The same logic was also used to formulate the recommendations and the funding, ownership and sustainability map.

Roadmap development

The evidence collected through document review, partner input, CA updates and follow-up project analysis was synthesised into the structure of this roadmap.
The cross-cutting sections identify mechanisms that should continue after CHESS, including lightweight coordination, targeted events, joint proposal preparation, continued staff exchange, ecosystem engagement, communication, exploitation and policy dialogue.
The Challenge Area sections then provide a thematic roadmap for each CA. They summarise the end-of-project status, key achievements, continuation priorities, planned actions, funding vehicles, cross-CA dependencies, indicators and main risks. This allows each CA to retain its specific focus while remaining aligned with the overall CHESS sustainability model.

The roadmap therefore combines two perspectives - a hub-level perspective, focused on cross-regional mechanisms, governance, funding, ecosystem engagement and visibility, and a Challenge Area perspective, focused on thematic continuation of research, pilots, tools, training and policy engagement.

This structure reflects the way CHESS has operated throughout the project: as a cross-regional collaboration framework supported by concrete thematic activities in the six Challenge Areas.

Limitations

The methodology is based primarily on project-internal evidence, partner input and available information on follow-up projects and proposals. As a result, some continuation pathways remain dependent on external decisions, especially the outcome of submitted funding proposals, national policy priorities, institutional resources and industry uptake.
The roadmap therefore avoids presenting all planned activities as guaranteed. Where funding is not yet secured or ownership is not fully defined, this is reflected as a dependency or risk. This approach is intended to make the roadmap realistic and useful for future coordination, rather than presenting a purely aspirational continuation plan.

4 End-of-Project Baseline: Where CHESS Stands Now

This section provides a concise overview of the main outcomes achieved within CHESS and their status at the end of the project. It summarises the key results across research, innovation, training and ecosystem engagement, focusing on their maturity and potential for continuation.

Over the course of the project, CHESS has delivered a broad portfolio of outputs across all six Challenge Areas. These include research and innovation activities implemented through mini-projects, the development of tools, pilots and demonstrators, training and mobility activities, as well as cross-sectoral community and dissemination efforts. In parallel, the project has successfully engaged with regional and European ecosystems, contributing to policy discussions and strengthening links with public authorities and industry stakeholders.

At the end of the project, these outputs show different levels of maturity and continuation potential. A number of tools, pilots and research activities are continuing through secured follow-up projects, particularly SECURE-NET, CCAT and QARC, or through national and institutional funding. Other activities remain at the stage of ongoing research or early validation and will depend on future funding, partner capacity or further development. In some cases, continuation is expected in a more limited or informal form through existing collaborations and network.

Overall, CHESS has evolved from a coordination and ecosystem-building initiative into a collaboration with concrete and partly sustainable outputs. These results provide a solid basis for further development and continuation beyond the project.

4.1 CHESS Mini-Projects

As of 2026, CHESS has transitioned from a networking initiative to a high-output research excellence hub. Strategic evaluation confirms a high level of maturity in the South Moravian and Estonian regions, marked by 25 initiated mini-projects. Of these, 11 have been completed and 14 are ongoing. More detailed information on all these mini-projects is in *D3.1 Mid-term evaluation report of CHESS R&I activities* and *D3.2 Report on Engagement of the Ecosystems into CHESS R&I.*

The full list of CHESS mini-projects, including their sustainability aspects, is provided in *Annex 1* at the end of this document.

4.2 Key Tools, Pilots, Methods, and Demonstrators

Our teams have been working on several solutions, improvements, and/or deployment of technologies, systems, or methods between sectors or regions. CHESS has produced a range of tools, pilots, and demonstrators across the six Challenge Areas, addressing topics such as security certification, post-quantum cryptography, blockchain security, software verification, and training infrastructure.

Several outputs have reached a level suitable for further adoption or piloting. For example, the sec-certs tool supports analysis of certification data, while post-quantum communication solutions have been tested in cross-regional pilots. In addition, training infrastructure and tools developed by teams involved in the project are already being reused in educational and practical settings.

More detailed descriptions of individual tools and demonstrators are provided in *Annex 2*.

4.3 Training and Mobility Results

Training and mobility activities within CHESS have played a key role in strengthening cross-regional collaboration, building competencies across sectors and enabling practical knowledge transfer between academia, industry and the public sector.

CHESS partners have organised a broad portfolio of training events, workshops and knowledge-sharing activities targeting diverse stakeholder groups, including students, researchers, industry professionals and public-sector representatives. These activities combined hands-on formats, such as cybersecurity exercises and training platforms, with more advanced expert-level workshops and conferences. By June 2026, we have presented CHESS results or trained different sectors at 139 events (training events, workshops, conferences, brokerage events, meetings with stakeholders).

Many of the training events were directly based on tools and methodologies developed within the project and were used both for skills development and for validating research results in real-world settings.

Mobility and staff exchange have further strengthened collaboration within the ecosystem. Fellowships between partners enabled direct knowledge transfer, joint research activities and closer integration between institutions across regions and sectors. These exchanges often led to follow-up collaborations, joint publications and new research directions, demonstrating their importance as a mechanism for sustaining cooperation beyond the project. By June 2026, we have supported 27 fellowships between Estonia and Czechia and at least another 6 are planned by the end of the project.

Overall, training and mobility activities have contributed not only to skills development but also to building a connected and active cross-regional cybersecurity community, providing a strong foundation for continued collaboration after the end of CHESS.

More detailed information on training and mobility activities for the first two years of the project is provided in *D2.1 Mid-term Report on Training and Mobility*. A comprehensive overview covering the second half of the project will be included in *D2.2 Final Report on Training and Mobility*, to be submitted by the end of 2026.

4.4 Community and Dissemination Results

CHESS organised a series of brokerage and networking events as key mechanisms for connecting stakeholders across academia, industry and the public sector, and for enabling follow-up collaboration. These events varied in format and target audience, reflecting the needs of different stakeholder groups.

The events highlighted in this section are not presented as a comprehensive overview of all dissemination activities, but as illustrative examples of those with the strongest impact on cross-regional collaboration. These activities went beyond standard dissemination and served as key mechanisms for building connections between stakeholders, enabling follow-up collaboration and demonstrating the practical relevance of CHESS results. As such, they provide evidence of a functioning and active collaboration ecosystem that will continue beyond the project lifetime.

In total, five brokerage and matchmaking events have been organised across Estonia and South Moravia so far, each bringing together between 40 and 80 participants from multiple countries and sectors. These events created opportunities to present project results, discuss emerging topics and establish new collaborations. Detailed information on these events is provided in *D3.2 Report on Engagement of the Ecosystems into CHESS R&I*. The final brokerage event is planned for September 2026 in South Moravia and will connect people with a background in cybersecurity, representing various sectors (academia, industry, government) from the Czech Republic and Estonia.

CHESS has also contributed to high-level visibility and strategic engagement. The project played an active role during the state visit of the President of the Czech Republic, Petr Pavel, to Estonia in May 2026. As an established platform connecting partners across Estonia and South Moravia, CHESS served as a concrete example of long-term cross-border cooperation in cybersecurity. As part of the official programme, CHESS partners from the University of Tartu and Cybernetica facilitated a business delegation meeting, bringing together around 40 representatives of Czech and Estonian cybersecurity stakeholders from academia, industry and the public sector. The discussions focused on ongoing collaboration and follow-up initiatives, including SECURE-NET, CCAT and QARC.

Another example of a targeted, practice-oriented activity is the CHESS Demo Day organised by the Estonian Information System Authority (RIA / NCSC-EE) in March 2026. The event showcased practical tools and solutions developed within CHESS and demonstrated their applicability in real-world settings, particularly for public-sector organisations. It provided a platform for direct interaction between researchers, cybersecurity professionals and policy actors.

Beyond events organised within the project, CHESS partners actively contributed to a wide range of conferences, workshops, seminars and stakeholder meetings, further

strengthening connections across the quadruple helix and increasing the visibility of the project results.

The CHESS website and social media channels have supported continuous dissemination and outreach. As of June 2026, the CHESS LinkedIn profile has over 2,300 followers, with additional audiences reached through X, Facebook and YouTube. These channels will remain important for maintaining visibility beyond the project lifetime.

Further details on communication and dissemination activities, including those planned after the end of CHESS, are provided in *D4.1 Dissemination, Exploitation and Communication Plan Update.*

4.5 Joint Proposals and Follow-up Projects

We have submitted six international research proposals of which three have been funded and all three are led by CHESS partners.

SECURE-NET (Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands, ID 101217315): ERA Talents including 11 partners, coordinated by the University of Tartu in Estonia, boosts industry-academia mobility among the CHESS regions and beyond, with Lithuania, Netherlands and Ukraine. CHESS partners included: UTARTU, MUNI, RIA, CYBER
https://securenet.isk.ktu.lt/

CCAT (Cybersecurity Certification and Assessment Tools, ID 101225878): The consortium of 9 institutions, coordinated by Masaryk University from South Moravia, universities and companies from the Czech Republic, Estonia, Italy and Germany. The project builds on four open-source cybersecurity tools developed in academia. The aim is to make them ready for use in applied, non-academic scenarios. CHESS partners included: MUNI, CYBER, UTARTU, Red Hat.
https://ccat.fi.muni.cz/

QARC (Quantum-Resistant Cryptography in Practice, ID 101225691): Project with 18 partners from 12 European countries, coordinated by Brno University of Technology from South Moravia (CHESS consortium member) QARC aims to enhance the transition to quantum-safe cryptography. As most of the current cryptosystems are vulnerable to attacks by quantum computers, the QARC project will provide methods, tools, and good practices based on post-quantum cryptography resistant to quantum threats. CHESS partners included: BUT, CYBER, MUNI, NÚKIB, Red Hat, RIA.
https://qarc.vut.cz/

Apart from these, several national grants have been submitted both in Czechia and Estonia. For example, the Czech project Cybersecurity Education and Training Research Center (CYBER-EDU, ID VL01010014) has recently been funded, involving Masaryk University, Brno University of Technology and NÚKIB. The project builds on CHESS activities in the area of cybersecurity training within Challenge Area 6 and will support their continuation. More detailed information on CA6 activities and their sustainability is provided in *Annex 1*.

4.6 Policy and Ecosystem Engagement

CHESS partners have actively engaged with public authorities and policy processes at both national and European level, contributing to alignment between research activities and policy and regulatory developments.

At national level, partners contributed to discussions on cybersecurity certification, post-quantum transition, and public-sector cybersecurity planning in both Estonia and Czechia. For example, Brno University of Technology contributed to NÚKIB recommendations on cryptographic means, a key document for compliance with national requirements. In parallel, discussions were held with NÚKIB and regional authorities in South Moravia on the potential use of the F4SLE framework, including its application for evaluating public-sector organisations such as hospitals.

In Estonia, Cybernetica and RIA were actively involved in the development of the national post-quantum cryptography roadmap published in 2026, while similar collaboration between BUT and NÚKIB is contributing to the preparation of the Czech national roadmap. CHESS partners have also contributed to certification-related policy discussions, with CYBER supporting national debates on certification of cryptographic systems and MUNI and BUT engaging with Czech authorities on certification of secure systems with cryptographic elements. CYBER and RIA are involved in a post-quantum transition project of the Estonian Population Registry, aiming to deliver a practical transition plan.

At the European level, CHESS engaged with key organisations including the European Cybersecurity Competence Centre (ECCC), European Cyber Security Organisation (ECSO), or European Network and Information Security Agency (ENISA), and thus contributed to broader ecosystem alignment. Also, CHESS has been assisting in pointing out deficiencies and in increasing transparency in product security certification schemes like Common Criteria and the EU Cybersecurity Certification Scheme on Common Criteria (EUCC) deployed across Europe. The follow-up project QARC further strengthens cooperation among national cybersecurity authorities, key industry and academic players in the area of post-quantum transition. CHESS results also feed into ongoing knowledge bases such as such as semi-annual RIA commissioned report on the lifecycle of cryptographic algorithms by CYBER. Finally, CHESS continues to support outreach and policy dialogue at European level, including planned events such as the Future Cryptography conference in Brussels in 2026, which will present project results to a wider policy and stakeholder audience.

5 Cross-Regional Roadmap for Post-Project Continuation

5.1 Roadmap Actions

This section presents the core continuation logic of the CHESS roadmap in the form of a set of cross-cutting actions. These actions translate the main continuation priorities identified in the project into concrete and implementation-oriented directions, combining both strategic focus and implementation mechanisms.

Action 1: Continue and scale research, innovation and exploitation activities

This action has two dimensions: 1) Consolidate and exploit CHESS outputs, 2) Continue selected R&I actions and pilots through follow-up projects.

Joint research and innovation activities remain a central element of continued cooperation between Estonia and South Moravia. Building on the results achieved within CHESS, partners will continue to develop selected research lines, pilots, and tools with the highest maturity and continuation potential. These activities include further development of cybersecurity tools and methods, implementation and scaling of pilot solutions, and validation of research results in real-world settings, and exploration of pathways to commercialization of most promising solutions. Particular emphasis is placed on activities that combine research excellence with practical applicability, including certification-related tools, post-quantum cryptography solutions, blockchain-based systems, and training infrastructures.

Implementation mechanism:

Our research and innovation activities will continue also thanks to the follow-up projects mentioned above. Concrete examples of continuing activities include further development and piloting of the sec-certs tool within the CCAT project, continued work on post-quantum communication and transition pilots within QARC, and the deployment of training platforms and cybersecurity exercises in educational and professional settings. Selected tools and methodologies, such as F4SLE, have been taken up by public-sector stakeholders and are being further applied and evaluated in national contexts. The PQC library has been used in the post-quantum electronic voting task and is also being integrated with other CYBER's projects in addition to CHESS. The secure communication channel software developed, deployed and tested by CHESS consortium partners is open-source and may be used for larger projects and solutions in PQC.

These examples reflect a broader pattern, i.e. CHESS outputs with clear ownership, identified users and follow-up funding show the strongest continuation and exploitation potential. The continuation model focuses on a number of mature and scalable activities, while allowing flexibility for new collaboration topics to emerge.

More specific information about continuation of work done within CHESS R&I mini-projects is included in *Annex 1*.

Action 2: Maintain and expand engagement within the CHESS ecosystem and beyond

To support the continued use uptake and development of CHESS results, we will remain connected to the wider innovation ecosystems in South Moravia and Estonia. The collaboration builds on the strong links developed within the consortium and beyond and will continue through participation in relevant platforms and networking activities connecting researchers, IT professionals, companies, and the public sector.

Partners will also build on existing ecosystem connections, including ITL and RIA in Estonia and JIC and NÚKIB in South Moravia, which play an important role in linking activities to regional innovation environments. These connections, as well as key industry-academic partnerships (CYBER-UTARTU, CYBER-MUNI, Red Hat – MUNI, Red Hat – BUT) will both exploit and strengthen transfer of ideas and new challenges to solve in various aspects of cybersecurity.

Building on this foundation, the CHESS network will remain open and continue to grow through follow-up projects and engagement with external stakeholders. This includes both strengthening existing collaboration links and gradually involving new partners and communities where there is clear thematic alignment. An overview of CHESS External Stakeholders relevant to our activities is provided in *D3.2 Report on Engagement of the Ecosystems into CHESS R&I*.

Implementation mechanism:

Partners will organise well-targeted events bringing together stakeholders from academia, industry, government, and civil society. These include conferences, workshops, and training activities focused on areas such as cybersecurity and post-quantum cryptography. We plan to continue organising different kinds of events, such as Future Cryptography Conference, ETACS and SP2I workshops, or post-quantum awareness and training workshops.

We will stay connected with the organisers of well-established platforms and conferences we have collaborated with to explore opportunities for further collaboration where relevant. This includes organisers of RIA CyberMeetUps in Tallinn, Küberinnovatsioon Conference in Tartu, Estonian Summer School on Computer and Systems Science (ESSCaSS), OpenSSL Conference and Information Security Summit in Prague, Velvet Innovation Conference in Brno, or the recently founded “cybersecurity event coordination board” for the South Moravian region under the umbrella of the South Moravia Innovation Center (JIC).

CHESS institutions will use new links created within the project when organising various events and will invite speakers from within the network where relevant.

Action 3: Maintain mobility, talent development and knowledge-sharing

Cross-border and cross-sectoral knowledge exchange has been organized within CHESS through short- and midterm mobility. This initiative has proven to be very valuable and has contributed significantly to building stronger collaboration links and capacity across regions and sectors.

Implementation mechanism:

Knowledge exchange will continue through staff exchanges and mobility schemes, in particular through the SECURE-NET project and complementary programmes such as Erasmus+. These mechanisms provide structured opportunities for researchers, students and professionals to engage in joint activities, share expertise and develop new collaboration lines.

The CHESS network established during the project will be actively used to support mobility and talent development. Existing partnerships and newly developed connections between institutions will facilitate continued exchanges, enabling students, early-career researchers and experienced professionals to participate in collaborative activities, training and research stays within the network. Knowledge sharing will also be reinforced through interaction with the wider ecosystem, including participation in selected collaborative activities and events (see Action 2 above).

Action 4: Strengthen policy engagement and cooperation with public authorities

CHESS partners will continue to work closely with public authorities at national and European level to ensure that project results remain relevant for policy and practice. The focus will be on areas where CHESS has already demonstrated impact, such as cybersecurity certification and post-quantum transition.

Cooperation with key stakeholders such as RIA and NÚKIB will continue through concrete activities, including contributions to national post-quantum roadmaps, certification-related discussions and public-sector use cases. Existing collaboration links will be further used to translate research results into practical applications and policy-relevant outputs.

Implementation mechanism:

Policy engagement will take place through direct collaboration with public authorities, participation in relevant initiatives and use of follow-up projects such as QARC and CCAT. These provide a framework for continued cooperation in areas such as post-quantum cryptography, certification and secure system deployment.

The collaboration will be based on practical use cases, pilot implementations and ongoing exchange of expertise. This ensures that policy engagement remains focused, relevant and directly connected to real-world needs.

More information about CHESS engagement in relevant policy discussions at both national and EU level is included in *D1.3 Action Plans for 6 CHESS Challenge Research Areas.*

Action 5: Develop joint proposals to European and national programmes

Building on the collaboration and experience gained within CHESS, partners will continue to prepare joint proposals for European and national funding schemes. The focus will be on projects that build on mature CHESS results and existing collaboration lines.

Implementation mechanism:

The CHESS network will be actively used to form new consortia and identify opportunities for follow-up funding. Existing partnerships provide a strong basis for identifying relevant topics and shaping competitive proposals. Grant offices involved in the project will continue to collaborate closely, sharing information on relevant calls and supporting proposal preparation. Mainly, funding experts from MUNI and UTARTU will regularly scan available opportunities.

Exchanging knowledge in research management, both in pre-award and post-award phases, has been a significant benefit of the CHESS project. Research managers have established strong working relationships through direct interaction, mutual visits and staff exchanges, resulting in well-connected support network across CHESS institutions. This network continues to expand into follow-up projects, where managers maintain active communication and knowledge sharing.

Also, Masaryk University is preparing new measures aimed at increasing the success rate in competitive funding schemes and supporting researchers in coordinator roles, for example through enhanced in-house advisory support. These developments are expected to benefit not only MUNI teams but also the wider CHESS collaboration network.

Action 6: Maintain visibility and continue communication activities

Maintaining visibility of CHESS results and ongoing collaboration is essential for their continued use, uptake and further development. Communication activities will therefore continue across CHESS and its follow-up projects.

Implementation mechanism:

Communication will be coordinated across CHESS and related initiatives, with continued use of established channels such as the CHESS website and social media, complemented by communication activities of follow-up projects.
Activities and outputs will be cross-linked across CHESS, SECURE-NET, CCAT and QARC to ensure continuity of visibility and to highlight the connections between project results and follow-up initiatives.

Communication teams will remain in close contact, regularly sharing content and coordinating activities where relevant. This approach enables consistent messaging while allowing flexibility for project-specific communication formats and audiences.

More information about dissemination, exploitation and communication activities after CHESS is included in *D4.1 Dissemination, Exploitation and Communication Plan Update*, in *Section 6 Dissemination and Exploitation Activities After CHESS*.

Overall, the continuation of CHESS will rely on a flexible model based on existing relationships, ongoing activities and follow-up projects. No new formal structures are planned after the end of the project; instead, collaboration will continue on a voluntary basis through established networks and partnerships.

A significant part of the joint work will naturally evolve within follow-up projects such as CCAT, QARC and SECURE-NET, which provide a practical framework for continued collaboration, knowledge exchange and further development of CHESS results.

Beyond these secured activities, the consortium is also exploring opportunities for a broader continuation of the CHESS collaboration. A potential “CHESS II” project is being discussed, with the aim of expanding cooperation beyond Estonia and South Moravia to additional European regions. The coordinator has initiated discussions with potential partners across Europe to identify suitable consortium configurations. The preparation of such a follow-up initiative will depend on the availability of an appropriate funding call.

At the same time, several national project proposals building on CHESS results are being prepared in both regions.

This combined approach ensures continuity while preserving flexibility and allowing the collaboration to evolve based on emerging opportunities and needs.

5.2 Main Risks and Funding Dependencies

The continuation of CHESS activities is subject to several risks and dependencies.

A key dependency is the availability of follow-up funding. Continued collaboration and further development of results will rely on funding from European programmes (e.g. Horizon Europe, Digital Europe), national schemes, and, where relevant, private sector engagement.

Mitigation: To mitigate this risk, partners will actively pursue diversified funding sources. Grant offices involved in the consortium have been working closely and will continue to do so in future. Existing follow-up projects also provide a partial continuation framework.

Several risks relate to the sustainability and practical use of project outputs. These include unclear ownership and long-term maintenance of developed tools, as well as the possibility of only partial funding for further development and deployment of research and innovation pilots.

Mitigation: Partners will clarify ownership and responsibilities for key outputs where relevant and build continuation into follow-up projects. Where full continuation is not secured, outputs will be maintained at a level that allows further development when new

opportunities arise. Open-source approach, inviting broader (than consortium members only) participation in further development of some project outputs will be utilized where possible.

Industry engagement also remains a challenge. Limited participation or uptake by industry partners may occur if financial incentives or operational benefits are not sufficiently clear.

Mitigation: CHESS partners will continue engage industry stakeholders through targeted events, pilots, and direct collaboration, focusing on practical use cases and clearly communicated benefits. Follow-up projects also provide opportunities to strengthen industry involvement.

At the ecosystem level, there is a risk of fragmentation of activities over time, particularly as follow-up projects may evolve in different directions. The continuation of collaboration also depends on the active involvement of key partners and individuals; changes in priorities or limited capacity could affect engagement.

Mitigation: Continued communication, joint activities and shared platforms will help maintain alignment across partners and challenge areas. The use of lightweight informal coordination mechanisms allows flexibility while preserving connections between activities.
External factors may also influence the impact of CHESS outcomes. These include regulatory and standardisation uncertainty, as well as resistance to updating established frameworks such as Common Criteria, which may slow down innovation.

Mitigation: CHESS partners will remain engaged in relevant policy and standardisation discussions at national and EU level, contributing their expertise where possible and aligning activities with emerging frameworks to the extent feasible.

Finally, there is a risk of reduced visibility of CHESS and its results after the end of the project, especially if communication activities are not sufficiently maintained across the network.

Mitigation: Communication activities will continue through follow-up projects and existing channels. Cross-linking of websites and social media, as well as coordination between communication managers, will help maintain visibility of CHESS results and ongoing activities.

5.3 Governance and Coordination

The Cybersecurity Excellence Hub developed within CHESS provides a strong foundation for sustained cross-regional collaboration, knowledge sharing and application-oriented activities.

To maintain active connections within the community, CHESS partners will continue to use lightweight coordination tools. This will include maintaining an updated mailing list and regular updates from the dissemination and communication lead (UTARTU), shared at

least twice a year. These updates will cover developments in follow-up projects, new collaboration opportunities and selected events.

Sustainable governance

After the end of CHESS, the formal project governance bodies will not continue in their original form. Cross-regional coordination will be maintained through a lightweight continuation model based on existing partnerships, secured follow-up projects and targeted information exchange. The main practical coordination mechanisms will include:

- an updated CHESS contact list maintained by the dissemination and communication lead;
- utilising the CHESS website and LinkedIn profile to share information on follow-up activities, events and funding opportunities;
- ad hoc coordination meetings linked to SECURE-NET, CCAT, QARC and future joint proposals;
- continued involvement of associated partners and public authorities where their expertise is relevant to specific outputs, policy discussions or dissemination activities;
- annual informal review of the continuation status of major CHESS outputs and cooperation lines.

Decision-making after CHESS will be activity-based rather than hub-wide. Each follow-up activity will be led by the partner or project responsible for the relevant output, while the broader CHESS network will serve as a pool of expertise, partners, users and dissemination channels.

6 Challenge Area Roadmaps

The previous section presented the roadmap as a set of cross-cutting actions defining how the CHESS collaboration will continue beyond the project. These actions focus on shared mechanisms such as research continuity, ecosystem engagement, mobility, policy interaction and proposal development.

This section complements that view by focusing on the six Challenge Areas, where the actual research and innovation activities take place. Each Challenge Area roadmap reflects its specific results, continuation priorities and planned activities, providing a more detailed and thematic perspective.

6.1 Challenge Area 1: Internet of Secure Things

Leading institutions: UTARTU, BUT
Other institutions involved: MUNI, CYBER, RIA

Current status at the end of CHESS

- Completed mini-projects: CA1_01 Empirical Research of Information Security and Privacy Management in Intelligent Infrastructure Systems; CA1_02 Analysis of Security-Aware and Privacy-Preserving Smart Parking Solutions; CA1_03 Secure and Privacy-preserving Access to Sharing Vehicles in Smart Cities; CA1_04 Security Risk Management in Automated Systems and Technology;
- Ongoing mini-projects: CA1_05 Security and Privacy in Teleoperated Systems.

Key achievements relevant to cross-regional collaboration

- Involved in CA1_03: BUT, UTARTU, MUNI, CYBER.
- Involved in CA1_04: UTARTU, BUT, RIA, MUNI.
- Involved in CA1_05: UTARTU, BUT.
- The use of focused mini-projects enabled partners to move efficiently from strategic alignment to tangible joint work.
- Within CA1, there have been multiple cross-regional fellowships organised in 2025 and 2026.
- CHESS partners have organized the Workshop on Security and Privacy in Intelligent Infrastructures (SP2I) co-located with ARES in 2023, 2024, 2025 and 2026.

Continuation priorities

- Security and privacy in teleoperated systems.
- Security risk management in automated systems and technology.
- Manage, analyse and design Internet of Secure Things systems.
- Resolving conflicting goals of forensic readiness and privacy; Validate in various sectors: smart cities, smart transportation, intelligent infrastructure in industry.

Planned actions and milestones (after CHESS ends)

- The cooperation activities regarding the mini-projects CA1_4 and CA1_5 and others are planned to continue beyond the completion of the CHESS project within following HE projects such as the supported SECURE-NET project or potentially in other projects submitted to Horizon Europe funding scheme.
- CA1 partners have submitted four follow-up EU projects that are related to IoST and other subtopics in area IoT. Depending on the outcome of these proposals, further submissions building on CHESS results may follow.
- CA1 plans to prepare and organize the International Workshop on Security and Privacy in Intelligent Infrastructures co-located at ARES.
- CA1 will also participate in and contribute to ETACS workhop, F4SLE seminars, and RIA Cyber MeetUps.
- CA1 partners plan to cooperate on common papers targeting conferences ARES, CAISE, and SECRYPT.

Cross-CA dependencies

- CA1 plans to cooperate with other CAs on multidisciplinary topics.
- Concretely, applying decentralised trust model based on blockchain into secure use cases of Internet of Secure Things such as cloud-based intelligent infrastructure processes or into the privacy-preserving car sharing scenario (CA4).
- Moreover, we expect that PQC algorithms (CA5) will be more deployed into CA1 security solutions.
- Close collaboration with CA2 supports the development of IoT-specific certification frameworks.
- Leveraging user-centric approaches from CA6 improves privacy and usability.

Funding/continuation vehicle

- Supported SECURE-NET project.
- More proposals planned.

KPIs and success indicators

- The success of CA1 will be measured through key metrics, including the number of industry partners engaged, the adoption of frameworks in real-world applications, and the impact of research outputs such as publications and presentations.
- Feedback from pilot projects will inform iterative improvements.

Main risks

- Limited industry engagement due to unclear financial incentives and operational benefits.
- Diverse security and privacy requirements across IoT applications complicate standardization.
- Difficulty attracting young researchers due to the competitive IT job market in Estonia and South Moravia.
- Funding status of submitted follow-up proposals is not yet secured.

6.2 Challenge Area 2: Security Certification

Leading institutions: MUNI, CYBER
Other institutions involved: Red Hat, RIA, UTARTU, CSH

Current status at the end of CHESS

- Ongoing mini-projects: CA2_01 Enriching Certification Report Analysis with other Open Source Intelligence; CA2_02 Testing the Method for Evaluating Organisations' Information Security Level; CA2_03 Common Criteria Protection Profile for Secure Computing Applications as PETs.
- The CA2 team has further developed sec-certs.
- We have been improving and testing a tool for online self-assessment of the information security level of organisations from different sectors both in Estonia and South Moravia.
- F4SLE was updated at the start of 2025. It has been piloted within various Estonian institutions and presented at various events in Europe and in Latin America.

Key achievements relevant to cross-regional collaboration

- Core sec-certs development is at this moment done at MUNI in close collaboration with Red Hat with additional cooperation and feedback from NÚKIB, CYBER and RIA.
- F4SLE has been translated into English, Spanish and Czech.
- In September 2025, we organised a workshop at NÚKIB with several representatives of constituents to explore the possibility of using F4SLE in Czechia.

- CA2 has organised several fellowships during the CHESS project.
- The Future Cryptography Conference 2025 was focused on the topic of certification with speakers from the project side, national stakeholders, ENISA, and contributors to NIST and ISO/IEC standards.

Continuation priorities

- Increase trust among end-users by using security certification to ease adoption of complex technologies, products and services.
- Structure certification documents for easy semi-automated processing to explain vulnerabilities and increase transparency in the certification process.
- Develop lightweight and automated recertification processes for institutions.
- Develop security certification labels for devices, software and organisations that provide a simple and unambiguous depiction of the levels of the security being certified.

Planned actions and milestones

- Mini-project CA2_01 will continue as part of the CCAT project started in 2026. In this project, MUNI, CYBER, Red Hat, UTARTU and RIA will pilot the use of sec-certs within CYBER and Red Hat, plus 2 external partners.
- Mini-project CA2_02 is used by RIA as part of national activities.
- RIA and UTARTU will share knowledge on F4SLE deployment in Estonia with NÚKIB and MUNI in order for NÚKIB to evaluate applicability in Czechia. Small-scale pilot will be undertaken in 2026 with South-Moravian hospitals.
- The results of mini-project CA2_03 will be used for certifying CYBER's secure multi-party computation platform.
- We plan to continue in exchanging staff also thanks to SECURE-NET project.

Cross-CA dependencies

- We will strengthen collaboration with other CHESS Challenge Areas, such as CA1, to develop certification frameworks tailored to interconnected devices.
- CA5 ensures quantum-resistant technologies are incorporated into certification processes.
- CA6 contributes to keeping tools accessible and user-friendly.

Funding/continuation vehicle

- CCAT project: secured.
- RIA national activities for F4SLE.

- CYBER innovation fund for further development and maintenance of the security target.
- SECURE-NET project for staff exchange: secured.

KPIs and success indicators

- The success of CA2 will be measured by the adoption of tools like sec-certs and F4SLE, the integration of vulnerability data into certification processes, and the broader application of the Common Criteria Security Target across industries.
- Advocacy outcomes, such as endorsements from certification bodies, will further demonstrate CA2 effectiveness.

Main risks

- Resistance to updating established certification frameworks, such as Common Criteria, creates barriers to innovation.
- Limited engagement with key decision-makers complicates progress.
- The labour-intensive nature of certification processes hampers their ability to respond swiftly to emerging threats.
- Creating a comprehensive PP is beyond the resources and time available in this project.

6.3 Challenge Area 3: Verification of Trustworthy Software

Leading institutions: MUNI, TalTech.

Other institutions involved: BUT, Red Hat, CYBER

Current status at the end of CHESS

- Ongoing mini-projects: CA3_01 The Deployment of Program Analysis Techniques to Practical Software Development; CA3_02 Development of Theory and Tool Support for Cybersecurity Protocols; CA3_03 Emerging Problems in Formal Methods.

Key achievements relevant to cross-regional collaboration

- Involved in CA3_01: MUNI, BUT, Red Hat, CYBER.
- Involved in CA3_02: CYBER, TalTech.
- Involved in CA3_03: MUNI, BUT, Red Hat, CYBER.
- CA3 teams have organised several events targeted at different sectors, especially bringing together researchers in academia with colleagues from industry, with a

focus on companies operating in Estonia and Czechia. The goal was to strengthen industry collaborations through initiatives like Industrial Days.

Continuation priorities

- Make use of Program Analysis Techniques to improve Software Development.
- Develop a theory of composable cybersecurity protocols to offer visual accounts of organisational cybersecurity protocols understandable to non-experts.
- Identify practically motivated challenges for basic research not yet covered by existing methodologies.

Planned actions and milestones

- We will continue with our three long-term mini-projects above and define new short-term priorities for each of them.
- It is likely that all mini-projects will be continued after the end of CHESS in the framework of follow-up projects.
- Recent advances in the synthesis and adaptation of randomized patrolling strategies enable their practical deployment for protecting critical infrastructure and other sensitive areas. Building on this, the CA3 team plan to continue this work and develop a software solution supporting the design, execution and adaptation of randomized patrolling strategies.
- Intensify activities in technology transfer.

Cross-CA dependencies

- We plan to collaborate with other Challenge Areas, for example, working with CA2 on integrating software verification techniques into certification frameworks and with CA5 on testing cryptographic protocols in post-quantum environments.

Funding/continuation vehicle

- Follow-up projects: awaiting results of submitted project proposals.

KPIs and success indicators

- Metrics for evaluating CA3 success include the adoption of tools like Symbiotic, the number of publications and conference presentations generated from its research, and the level of industry engagement in collaborative projects.
- Feedback from initiatives such as Industrial Days will further inform the effectiveness of outreach and knowledge transfer efforts.

Main risks

- Lack of funding; at the moment, we are still waiting for the results of the submitted project proposals.

6.4 Challenge Area 4: Security Preservation in Blockchain

Leading institutions: UTARTU, MUNI

Other institutions involved: BUT, Guardtime, CYBER

Current status at the end of CHESS

- Completed mini-projects: CA4_1 Automated trust through self-sovereign identity in the data exchange systems; CA4_02 Emergency Information Transmission Using Blockchain in Intelligent Vehicular Communication; CA4_03 Blockchain-Related Operation Protected by Cryptographic Hardware; recently completed mini-project CA4_04 Security risk management of intelligent infrastructures using blockchain.
- Ongoing mini-projects: CA4_05 Privacy of blockchain transactions; CA4_06 Methods for More Compact and Secure Blockchains; CA4_07 Blockchain-based intelligent infrastructures.

Key achievements relevant to cross-regional collaboration

- Involved in CA4_05: MUNI, UTARTU, BUT.
- Involved in CA4_06: MUNI, UTARTU, BUT, Guardtime, CYBER.
- Involved in CA4_07: UTARTU, BUT.
- The threshold cryptography demonstrator with MeeSign platform extended as part of CA4 was included at the RIA for demo day dissemination event in March 2026 in Tallinn.
- There have been multiple cross-regional and cross-sectoral fellowships organised.

Continuation priorities

- Illustrate the state-of-the-art use of blockchain in vehicular communication environment.
- Develop building blocks for hardware wallets with multiparty computation.
- Investigate privacy enhancing technologies used in Bitcoin blockchain.
- Security Risk Management of Intelligent Infrastructures using Blockchain.
- Privacy of Blockchain Transactions.
- Methods for More Compact and Secure Blockchains.

Planned actions and milestones

- All three currently running mini-projects will continue beyond the completion of the CHESS project with expanded scope.
- CA4_05 Privacy of blockchain transactions: the funding is only partly secured as the EU project submitted on this topic was not funded. Additional cooperation with CYBER on Sharemind-based CoinJoin protocol was started.
- Part of CA4_06 focused on analysis of cryptographic implementations will continue after CHESS with financing through the CCAT EU project.
- CA4_07 progress will continue after CHESS with financing through the SECURE-NET EU project.
- Extension of pressto analysis robot is included in project proposal submitted under Czech Ministry of Interior funding call.

Cross-CA dependencies

- We plan to scale pilot projects applying blockchain-based solutions to intelligent transportation and critical infrastructure sectors.
- CA1 could integrate blockchain for data integrity.
- CA5 provides quantum-resistant cryptographic technologies critical for securing blockchain systems.
- CA6 will collaborate with CA4 to build user trust and understanding of new systems and tools.

Funding/continuation vehicle

- CCAT project for part of CA4_06: secured.
- SECURE-NET project for CA4_07: secured.
- Czech Ministry of Interior proposal for pressto analysis robot: submitted.
- CA4_05 continuation: industry funding of phd student; EU project not funded; options for resubmission are investigated.

KPIs and success indicators

- CA4 success will be measured through the adoption of tools, interest in research analyses, and new research cooperations resulting in quality scientific publications.

Main risks

- The funding is only partly secured as some EU project submitted were not funded.

6.5 Challenge Area 5: Post-Quantum Cryptography

Leading institutions: CYBER, BUT

Other Institutions involved: Red Hat, NÚKIB, MUNI, RIA

Current status at the end of CHESS

- Completed mini-projects: CA5_02 Implementation of transition to post-quantum technologies.
- Ongoing mini-projects: CA5_01 Aspects of transition to post-quantum technologies; CA5_03 (Post-)Quantum Communication Infrastructure Pilot.

Key achievements relevant to cross-regional collaboration

- The series Future Cryptography Conference was created as part of CHESS to disseminate the project results at the national and international level.
- Student internships between BUT and CYBER, mainly to realize the PQC VPN Pilot.
- Staff internships between BUT and CYBER, mainly to compose consortia and create proposals for next projects.
- Close collaboration between NÚKIB and RIA authorities in road mapping post-quantum transition.
- Software-based and hardware-based pilots of quantum-secure communication link between Estonia and Czechia.

Continuation priorities

CA5 priority is continuous work on post-quantum transition, including updating the roadmaps according to the future information, piloting the transition steps in real organizations, and disseminating the best practices, specifically:

- Evaluate the current state and practical applicability of post-quantum technologies.
- Assess usability and market viability of information security products based on post-quantum algorithms.
- Contribute to the PQ transition roadmaps.
- Conduct pilots in PQ transition of the public and private sector organizations.
- Address non-technical aspects of transition to post-quantum technologies.
- Develop and deploy PQC encryptors.
- Continue research and development in new post-quantum technologies and deployment patterns; development of new PQ cryptographic primitives for advanced applications (zero-knowledge proofs, Internet voting protocols, etc.); improving the implementations (both soft- and hardware) of post-quantum algorithms.

Planned actions and milestones

- The example is a new HEU project QARC. This project started on January 1st, 2026, and it will directly build on the results obtained in CHESS, heading more towards specific pilots.
- A new HEU project MESAQ focused on hardware implementations has been submitted to the 2026 HEU calls and multiple projects on PQC will be submitted to national calls in 2026.
- CHESS CA5 topics have been covered during the RIA cyber meetups, and this tradition is expected to carry on in 2026 and beyond.
- We will continue to organize PQC workshops in future, as the general knowledge about PQC is still relatively low.
- Cybernetica and RIA are actively engaged in the development of the PQC roadmap for the Estonian state. BUT and NÚKIB are also collaborating on Czech national roadmap which is planned for 2026.

Cross-CA dependencies

- We plan to collaborate with CA1 to integrate quantum-safe protocols into IoT systems and with CA2 to align certification frameworks with emerging post-quantum standards.
- CA5 quantum-resistant cryptographic technologies critical for securing blockchain systems.

Funding/continuation vehicle

- QARC project: secured.
- Multiple projects on PQC will be submitted to national calls in 2026: planned.

KPIs and success indicators

- The success of CA5 will be measured by the adoption of its PQC library, the number and impact of publications, and the outcomes of pilot implementations in authentication, encryption, and VPN use cases.
- Additional metrics include the integration of quantum-safe protocols into real-world systems and the establishment of partnerships with industry and government stakeholders.
- For awareness and training sessions, the number of attendees is an indicator.

Main risks

- As the piloting activities revealed some shortcomings in the software implementation of the post-quantum encryptors that caused problems in long-distance data transfers, these weaknesses had to be fixed.
- The general knowledge about PQC is still relatively low.
- The adoption of PQC technologies is still very low, but the pace is increasing.

6.6 Challenge Area 6: Human-Centric Aspects of Cybersecurity

Leading institutions: MUNI, TalTech

Other institutions involved: UTARTU, RIA, NÚKIB, CYBER, Red Hat

Current status at end of CHESS

- Completed mini-projects: CA6_01 Hands-on Cybersecurity Training.
- Ongoing mini-projects: CA6_02 Improving the usability of penetration testing reports; CA6_03 Delivering Tabletop Exercises.

Key achievements relevant to cross-regional collaboration

- The MUNI team hosted two workshops, one in Tallinn and one in Tartu, to introduce the work to companies and government institutions, and get feedback. Around 40 people participated in the two events combined.
- The CA6 lead stayed in Estonia for one week, presenting the INJECT exercise platform at different institutions and discussing possibilities for new collaborations.
- The CA6 team at MUNI held the first training event for trainers, introducing the INJECT exercise platform to local stakeholders from industry and project partners in the Czech Republic.
- MUNI Fellowship in Estonia (2025): The fellowship enabled the deployment of the INJECT platform at Tallinn University of Technology (TalTech) and the development of a tabletop exercise for the maritime domain.
- TalTech Fellowship at Masaryk University (MUNI) (2025): The fellowship focused on testing and evaluating the previously developed tabletop exercise.

Continuation priorities

- Research on hands-on training as a key method to empower cybersecurity professionals and ordinary users with the skills needed to strengthen resilience and support effective incident response.
- Emphasis on usable security, focusing on making security tools and processes user-friendly – with a particular focus on the usability of penetration testing reports.

- Design, delivery, and assessment of tabletop exercises using AI.
- Improving the usability of penetration testing reports.

Planned actions and milestones

- We will continue with testing the newly created CHESS exercises and refine them based on feedback from initial runs.
- We will also explore the potential of using generative AI for exercise design and development.
- Additional workshops will be organized for users interested in the INJECT platform and digital tabletop exercises.
- We plan to introduce the INJECT platform and the newly developed tabletop exercises to teachers from Estonian vocational schools as well as general education schools during the Summer Schools 2026.
- We will use the INJECT platform to deliver a cybersecurity workshop at the CyberWizards 2026 camp. The platform will enable participants to engage in hands-on cybersecurity exercises and realistic challenge scenarios, supporting the practical learning approach central to the camp's 2026 educational program.
- A cybersecurity bootcamp is scheduled for August 2026, involving 35 young cyber talents. During the event, participants will use the INJECT platform to enhance their cybersecurity skills and knowledge while collaboratively designing and developing new tabletop exercises.
- CA6_02 will most likely organize more workshops or knowledge-transfer inputs to other events like DevConf or RIA CyberMeetup.

Cross-CA dependencies

- We will collaborate with CA1 and CA4 to build user trust and understanding of new systems and tools.
- We will work to bridge the gap between certification frameworks (CA2) and practical implementation by making certification processes more accessible and user-friendly.

Funding/continuation vehicle

- CA6_03 will continue within the Czech national project VL01010014, Cybersecurity Education and Training Research Center (CYBER-EDU). The project will start in September 2026, will be led by MUNI, and will also involve BUT, and NÚKIB. It will be funded by the Ministry of the Interior of the Czech Republic for the period from September 2026 to December 2030.
- CA6_02 may in some form continue, depending on industry collaboration.

KPIs and success indicators

- Metrics for evaluating CA6 success include the number of participants in training programs and tabletop exercises, feedback received, and measurable improvements in cybersecurity awareness and preparedness.
- Additional indicators include adoption rates of usability-enhanced tools and systems, as well as stakeholder engagement levels across sectors.

Main risks

- CA6_02 may in some form continue, depending on industry collaboration.
- CA6_03 – Although the project has successfully attracted participants to tabletop exercises, there is a risk that the broader adoption of INJECT-based exercises will remain limited. Many organizations face resource constraints and competing priorities, which hinder their ability to integrate these activities into their regular training practices, despite the reduced barriers to entry.

7 Lessons Learned on Cross-Regional Collaboration

7.1 What Worked

Lessons learned from the implementation of CHESS activities were previously analysed in Deliverable *D1.3 Action Plans* (December 2025). This section builds on those findings and provides a consolidated and updated overview, reflecting both earlier insights and additional experience gained during the later stages of the project.

1. **Collaboration built around concrete, well-defined activities**

Experience from the project confirmed that collaboration is most effective when structured around clearly scoped and well-defined research and innovation activities that are relevant to all partners involved. The use of focused mini-projects allowed participants to move efficiently from initial alignment to hands-on joint work, delivering tangible results without unnecessary organisational complexity. The combination of the mini-project approach with follow-up funding mechanisms further supported the transition of results beyond isolated outputs towards longer-term development.

2. **Fellowships and mobility as key enablers of collaboration**

Fellowships and mobility schemes were highly effective in fostering cross-regional and cross-sectoral collaboration. They supported knowledge exchange not only at the individual level but also at institutional level, as visits were typically complemented by seminars, workshops, or teaching activities. Most fellowships had a strong cross-sectoral dimension, benefiting from the close proximity of universities to non-academic CHESS partners. At the same time, experience showed that for some challenge areas, organising longer stays remains more demanding.

3. **Embedding activities in existing ecosystems**

Experience from the project showed that linking CHESS activities to established regional, national and European ecosystems significantly enhanced their visibility and overall impact. Organising events in connection with existing conferences and community platforms consistently led to higher participation and stronger integration with relevant cybersecurity communities compared to standalone formats.

In addition, targeted outreach to external stakeholders proved to be an effective approach. This highlighted the importance of tailoring event formats, content and communication channels to specific audiences in order to ensure relevance and maximise engagement.

4. **Early planning for sustainability and follow-up funding**

Planning for sustainability and follow-up funding early in the project proved to be an important factor for ensuring continuity beyond the CHESS timeline. The involvement of

institutional grant offices supported timely preparation of continuation proposals and helped translate ongoing collaboration into concrete follow-up initiatives.

5. **Active involvement of public authorities**

Project experience confirmed that close engagement with public authorities increases both the relevance of activities and the likelihood of uptake of project results. Cooperation with national cybersecurity authorities enabled early exchanges on the practical applicability of selected tools and approaches, and supported alignment of activities across regions as well as coordinated dissemination efforts.

6. **Academic–industry cooperation**

Close cooperation between academia and industry across several challenge areas proved beneficial. For example, the sec-certs framework has been tested beyond the CHESS consortium and is being taken up by external commercial organisations, with further development continuing in the follow-up project CCAT. Dedicated formats such as Industrial Days facilitated knowledge exchange, although feedback from stakeholders indicates that clearer incentives are needed to motivate broader participation in pilot deployments and solution adoption.

7. **Research management strategies**

Two complementary approaches were particularly effective when it comes to research management and coordination. First, we organised one-on-one meetings between the coordinator and individual partners. These created a space for open discussion of challenges, plans, and support needs. This format allowed for targeted problem-solving and helped identify risks early on. Second, an informal peer-learning network of research managers at Masaryk University was created by the CHESS Project Manager at the beginning of the project. Initially established as a small support group, it grew organically into a regular platform connecting colleagues involved in Horizon Europe project implementation and coordination across different faculties and organisational units. This network enabled sharing of practical experience, mutual support, and improved consistency in project management, and continues to attract additional participants.

7.2 What Should Be Continued

1. **Sustaining and expanding mobility schemes**

The CHESS network will continue to be used to enable staff exchange beyond the project's lifetime. The new ERA Talents project SECURE-NET will further support structured industry–academia mobility within the CHESS regions and beyond.

2. **Leveraging established events and networks**

By scheduling our final and follow-up events alongside well-established conferences, community platform and ecosystem initiatives, we will maximise visibility, leverage existing

networks and foster new connections that will continue to benefit the CHESS community beyond the project's lifetime.

3. **Long-term funding strategy and consortium building**

To sustain collaboration and partnerships beyond the funded period, continued investment is essential. Grant offices across CHESS institutions will remain actively engaged in monitoring funding opportunities and supporting proposal development. The CHESS network will be used to form new consortia and maintain strategic continuity.

4. **Strengthening industry engagement and uptake**

Stronger and more structured engagement with industry partners is critical. Future activities should place greater emphasis on incentives for pilot testing, validation, and adoption of CHESS tools, inclusive of the pathways to commercialization and utilization of open-source adoption models.

5. **Contributing to research management culture at Masaryk University and beyond**

An informal platform connecting research managers across Masaryk University created at the beginning of the CHESS project has gradually developed into a regular forum for sharing practical experience and addressing implementation challenges (it now has 17 members). Given its usefulness and the growing interest among colleagues, this platform is expected to continue beyond the project as a lightweight mechanism for knowledge exchange, with potential for further expansion to additional areas and institutions.

7.3 What Did Not Work Well Enough

Not all collaboration mechanisms worked equally well. Industry engagement was strongest where partners could present concrete tools, pilots or demonstrators, but more difficult where the expected benefit for companies was less immediate or where participation required significant operational commitment. Some Challenge Areas also depended strongly on individual researchers or specific funding opportunities, which creates a risk for continuity after the end of CHESS. Longer mobility stays were valuable but not always easy to organise due to teaching duties, project commitments and institutional capacity. Finally, the maturity of outputs differs across Challenge Areas: while some tools already have clear continuation vehicles or adopters, others remain at the research, prototype or early validation stage.

8 Recommendations

The recommendations below translate the experience of CHESS into practical guidance for the post-project phase. They are addressed to the consortium, Challenge Area leaders, associated partners, regional ecosystems, public authorities and funders. Their purpose is not to create an additional governance layer, but to support continuity, ownership and uptake of results after the end of the project.

8.1 Recommendations for the Consortium

The consortium should maintain CHESS as a lightweight collaboration network rather than transforming it into a new formal structure. The most realistic continuation model is based on existing institutional partnerships, secured follow-up projects, targeted communication and ad hoc coordination around concrete activities. Embedding CHESS activities within existing ecosystems significantly increased their reach and impact.

The consortium should keep an updated contact list and use it for selective information sharing, including relevant events, funding calls, policy developments and opportunities for cooperation. A short newsletter or update prepared approximately twice a year would be sufficient to maintain visibility without creating unnecessary administrative burden.

For each major CHESS output, the consortium clarified ownership and maintenance responsibility. This is particularly important for tools, pilots, training materials and demonstrators that may continue to be used after the project. Where ownership is not yet fully defined, the responsible partners should agree whether the output will be maintained, further developed, transferred to a follow-up project, or archived as a completed research result.

The consortium should continue to use the CHESS network for proposal preparation. The experience gained through SECURE-NET, CCAT and QARC shows that early involvement of grant offices and clear thematic ownership significantly increase the chances of successful follow-up funding. Future proposals should build on mature CHESS outputs and avoid creating overly broad consortia without a clear continuation logic. The involvement of institutional grant offices will be the key here.

Communication and dissemination should continue through the CHESS website, social media channels and the communication channels of follow-up projects. CHESS results should be cross-linked with SECURE-NET, CCAT and QARC to preserve the visibility of the original hub and demonstrate its long-term impact.

8.2 Recommendations for CA Leaders

Challenge Area leaders should prioritise a limited number of realistic continuation actions rather than maintaining all activities at the same level. Each CA should distinguish between completed outputs, outputs ready for adoption or piloting, research lines requiring further development, and activities that depend on additional funding.

For each continuation action, CA leaders should define the lead partner, involved partners, expected users, funding status, next milestone and main risk. This will make the roadmap easier to monitor and will help future proposal preparation.

CA leaders should pay particular attention to the maturity and adoption pathway of their outputs. Research results and prototypes should be accompanied by clear use cases, target groups and validation needs. Tools and demonstrators should specify whether they are intended for further research, operational piloting, training, public-sector use, industry uptake or standardisation/policy input.

Cross-CA cooperation should focus on synergies that are already active or realistically actionable:

- CA1 IoT security frameworks must scale to larger applications, such as automated systems, through collaboration with industry and government stakeholders.
- CA2 tools like sec-certs and F4SLE should be prioritized for adoption as industry standards, modernizing certification frameworks.
- CA3 software verification tools need integration into industry workflows, supported by joint initiatives with developers.
- For CA4, blockchain pilots in IoV and critical infrastructure require further regulatory support to encourage adoption.
- CA5 work on post-quantum cryptography should transition to larger-scale testing and operational deployment.
- CA6 human-centric approach must continue to bridge the gap between technical advancements and user adoption, expanding training and usability studies to reach broader audiences.

CA leaders should also identify talent and capacity risks. Several CHESS activities depend on specific researchers, technical teams or institutional expertise. Future planning should therefore include staff exchange, junior researcher involvement, documentation of tools and methods, and integration of selected results into teaching and training activities.

8.3 Recommendations for Associated Partners and Regional Ecosystems

Associated partners and regional ecosystem actors should be involved selectively, where their role adds clear value. Their most important contribution after CHESS is not general

participation in the network, but targeted support for dissemination, validation, policy alignment, stakeholder access and uptake of specific outputs or specific cooperation in the form of planning joint events or contributing to events organised by these institutions and targeted at regional stakeholders.

Regional ecosystems in Estonia and South Moravia should continue to serve as entry points for external stakeholders interested in CHESS results. This includes companies, public-sector organisations, educators, community actors and potential adopters of tools, training formats or policy-relevant outputs.

The strong relationships we have been building during the CHESS project should form the basis for continued cooperation in the follow-up projects of CHESS, i.e. CCAT, QARC and SECURE-NET.

8.4 Recommendations for Public Authorities and Funders

Public authorities and funders are encouraged to use CHESS results as evidence of the value of cross-regional cybersecurity cooperation. The project demonstrated that targeted collaboration between research institutions, companies, public authorities and ecosystem actors can produce practical outputs.

Public authorities should consider where selected CHESS outputs can support national or regional cybersecurity priorities. This is particularly relevant for post-quantum transition planning, cybersecurity certification, organisational security self-assessment, public-sector training and the secure deployment of emerging technologies.

Funders should support continuation pathways that combine technical maturity, clear ownership and realistic adoption potential. Follow-up funding should prioritise activities that already have demonstrated cross-regional cooperation, identified users, credible lead partners and a clear sustainability plan.

Public authorities and funders should also support the connection between research outputs and policy or standardisation processes. Several CHESS results are relevant for EU-level and national discussions on cybersecurity certification, post-quantum cryptography, secure digital infrastructure and cyber resilience. Maintaining these links will increase the long-term impact of the project beyond the original consortium.

9 Conclusion

CHESS has created a durable basis for cross-regional cybersecurity cooperation between Estonia and South Moravia. Over the course of the project, the consortium moved from strategic alignment and ecosystem mapping to concrete research and innovation activities, pilot implementations, tools, training formats, mobility schemes, public-sector engagement and follow-up proposals.

The end of the CHESS project does not mean the end of the collaboration it created. Several continuation pathways are already secured through SECURE-NET, CCAT and QARC, while additional proposals and national activities provide further opportunities for development. At the same time, the roadmap recognises that not all activities will continue in the same form or with the same level of intensity. Some outputs are ready for further adoption or piloting, others require additional research, and some depend on future funding or institutional capacity.

The most realistic sustainability model for CHESS is therefore a lightweight and output-driven continuation model. Rather than creating a new formal structure, partners will maintain cooperation through existing relationships, follow-up projects, targeted communication, joint events, staff exchange, policy engagement and new proposal preparation. This model reflects the practical experience of the project and avoids unnecessary administrative complexity.

The roadmap also shows that the strongest continuation potential exists where three conditions are present: a concrete output or cooperation line, a clear owner, and a credible funding or adoption pathway. These conditions should guide the post-project phase and help partners prioritise activities with the highest potential impact.

CHESS has demonstrated that regional cybersecurity ecosystems can generate European added value when they combine technical excellence, public-sector relevance, industry engagement and sustained knowledge exchange. The task for the next phase is to preserve this momentum, keep the network active, and ensure that the most mature results continue to support cybersecurity resilience, innovation and policy development in Estonia, South Moravia and the wider European cybersecurity community.

Annex 1

This annex provides a detailed overview of all CHESS mini-projects, including their objectives, current status (completed or ongoing), and, where relevant, information on their continuation and sustainability beyond the project.

Challenge Area 1: Internet of Secure Things (IoST)

CA1_01 Empirical Research of Information Security and Privacy Management in Intelligent Infrastructure Systems

- This mini-project explored the current state of security and privacy management in intelligent infrastructure systems used in smart transportation sector in Estonia and South Moravia.
- Status: Completed

CA1_02 Analysis of Security-Aware and Privacy-Preserving Smart Parking Solutions

- This mini-project focused on researching secure and privacy-preserving solutions for vehicle parking solutions. The main objectives included (i) exchanging requirements and lessons learnt from the previous R&D activities, (ii) expanding a secure and privacy-preserving design, and (iii) exploring how to design security and privacy-preserving means into the parking scenario.
- Status: Completed

CA1_03 Secure and Privacy-preserving Access to Sharing Vehicles in Smart Cities

- The objective of CA1_03 is to explore different car-sharing scenarios. We plan to apply a security risk management approach to elicit security risks and their countermeasures and to design secure and privacy-preserving solutions.
- Status: Completed

CA1_04 Security Risk Management in Automated Systems and Technology

- The objective of CA1_04 is to explore security risks in automated systems and technologies, focusing on manufacturing systems. The expected result is a report that identifies and explains these cyber security risks, along with suggesting practical ways to reduce them. We aim to perform a few use-case analyses of the selected manufacturing systems.
- Status: Completed
- Sustainability: New EU proposals with UT and BUT on the board will focus on security in Operational Technologies (OT) and manufacturing systems.

CA1_05 Security and Privacy in Teleoperated Systems

- The objective of CA1_05 is to analyse different teleoperation scenarios, to determine protected assets and security risks and to elicit security countermeasures. We aim to design secure and privacy-preserving solutions for teleoperated systems.
- Status: Ongoing

- Sustainability: The cooperation between UT and BUT mainly aims at expanding the topic and future research activities, for instance, adding PQC into solutions (under QARC activities), and aligning with the conflicting goals of regulations and design solutions in collaboration with the UTARTU Autonomous Driving Lab.

Challenge Area 2: Security Certification

CA2_01 Enriching Certification Report Analysis with other Open Source Intelligence

- The team has researched and developed sec-certs, a tool aiming to support the certification of organisations and their information systems. Security certification frameworks like Common Criteria and FIPS 140 form a large landscape of thousands of certificates, security targets, and protection profiles. Using data mining and natural language processing, we developed insights into the dynamics of the certification ecosystem and the proactive analysis of the impact of past and possible future vulnerabilities. The expertise available within the CHESS project enabled us to improve the usefulness of analyses and features available to end-users and better assess the impact of certification rigour level on subsequent frequency and seriousness of the product vulnerabilities.
- Status: Ongoing
- Sustainability: CCAT project will provide both further challenges from new industry and certification ecosystem users, as well as financial support.

CA2_02 Testing the Method for Evaluating Organisations' Information Security Level

- Within this mini-project, we have been testing a tool for online self-assessment of information security level of organisations from different sectors both in Estonia and South Moravia, i.e. municipalities, private sector, healthcare, education, ICT, non-profit, government office, finance. The European NIS2 directive aims to enhance the security of the digital society by mandating the adoption of security measures by various sectors. To assess progress, systematic evaluation of security levels is crucial. F4SLE (the framework for security level evaluation), along with its updating method MUSE and presentation engine MASS, provides institutions with immediate feedback on their security status, enables benchmarking, and centralises aggregated data for comprehensive evaluation.
- Status: Ongoing
- Sustainability: RIA is taking over further maintenance and development of both the frameworks as well as supportive tools. MUNI and UTARTU will support selected activities through Master's theses.

CA2_03 Common Criteria Protection Profile for Secure Computing Applications as PETs

- We aimed to define a Common Criteria (CC) protection profile (PP) for secure computing applications as privacy enhancing technologies. We found in the initial research that creating a comprehensive PP is beyond the resources and time available in this project. We have since determined that a security target (ST) will help us achieve our goals more efficiently. We have determined the scope of the ST and gathered requirements and priorities from stakeholders. Our investigation led us to the decision to create two different STs for different technologies (secure multi-party

computation (MPC) and trusted execution environments (TEEs)). We estimate that, by the end of the project, the ST for MPC will be in a mature draft stage.
- Status: Ongoing
- Sustainability: CYBER will finalise, maintain and update the created ST after the end of the project. CYBER aims to certify its MPC platform w.r.t. to the created ST.

CA2_04 Security certifications issues with disk and storage encryption
- This mini-project is based on long-term disk development know-how (LUKS, VeraCrypt, BitLocker, and self-encrypting OPAL), focusing on the disk encryption commonly used in FIPS140/CC environment and utilizing the MUNI testbed of OPAL drives for analysis (~ 40 drives). We first focus on the AES-XTS IEEE standard going through important revision, introducing key scopes and very likely affecting all certified systems in the future. Planned research areas: 1) The XTS key scope reasoning is very weakly described; no other options are researched => we would like to analyse and propose alternatives and guidance for implementers (in cooperation with Red Hat). 2) Analysis of certification requirements (enforced limits) that changes security model (e.g., FIPS-140 induced changes in software diverting from common code base).
- Status: Completed.

Challenge Area 3: Verification of Trustworthy Software

CA3_01 The Deployment of Program Analysis Techniques to Practical Software Development
- This mini-project focuses on developing and testing advanced tools for software analysis in real-world environments. The work combines applied development of practical tools with fundamental research in program analysis and system behaviour. Existing tools such as DiffKemp and Perun are being extended and improved to support more efficient code validation and performance analysis, including applications in large-scale systems like the Linux kernel. Additional tools explore automated testing and advanced verification methods. Overall, the goal is to make advanced software analysis techniques more usable, scalable, and relevant for industry practice.
- Status: Ongoing
- Sustainability: Continuation is expected, but the extent will depend on the availability of follow-up funding. Where feasible, activities will continue, including close academia–industry collaboration, with an increased focus on technology transfer.

CA3_02 Development of Theory and Tool Support for Cybersecurity Protocols
- We are working on applying techniques from formal semantics of programming languages, in particular programme equivalence, and adapting them to the setting of cryptographic protocols. Rewriting techniques from programming language theory can be used to establish observational equivalence of cryptographic protocols up to probabilistic negligibility. This allows us to reason about whether two protocols are indistinguishable and preserve important properties such as privacy.
- Status: Ongoing (The mini-project is expected to be completed by the end of 2026.)

CA3_03 Emerging Problems in Formal Methods

- This mini-project focuses on developing methods for designing efficient and reliable control strategies for multi-agent systems. The work combines algorithm development with practical tools that help make complex system behaviour easier to understand. In particular, it addresses how to create strategies that remain robust even when some components fail, and how to visualise these strategies in a way that supports their practical use. A prototype visualisation tool has already been developed, showing the potential for real-world applications.
- Status: Ongoing
- Sustainability: Continuation depends on the availability of follow-up funding.

Challenge Area 4: Security Preservation in Blockchain

CA4_1 Automated trust through self-sovereign identity in the data exchange systems

- We explored the feasibility of a decentralised approach for organisations' identity management in data exchange systems. More specifically, we focused on the potential of implementing self-sovereign identity (SSI) concepts in data exchange systems and how it affects identity management. The mini-project focused on the case study of the X-Road system – a solution that acts as a data exchange layer and enables secure data exchange between organisations in the public and private sectors.
- Status: Completed

CA4_02 Emergency Information Transmission Using Blockchain in Intelligent Vehicular Communication

- The aim of the project was to develop a use case that combines the concept of a digital twin with blockchain-based Internet of vehicles (IoV) technology to monitor the pre-failure conditions of vehicles for their predictive maintenance.
- Status: Completed

CA4_03 Blockchain-Related Operation Protected by Cryptographic Hardware; recently completed mini-project

- This mini-project focused on the practical security of cryptographic signing devices relevant to blockchain operations, and the means of improve them using secure multi-party computation (MPC).
- Status: Completed

CA4_04 Security risk management of intelligent infrastructures using blockchain

- This mini-project focused on improving the security of information transmission in intelligent infrastructures, with an emphasis on the application of blockchain technology.
- Status: Completed

CA4_05 Privacy of blockchain transactions

- This mini-project focuses on improving privacy and security in digital transactions. It explores new approaches to electronic cash using secure hardware and multi-party

computation to reduce reliance on trusted components, and analyses privacy risks in blockchain-based mechanisms such as CoinJoin. The work combines practical experimentation with data-driven analysis and has already led to the development of tools and open-source implementations.

- Status: Ongoing
- Sustainability: The mini-project already resulted in two published articles and two more currently in a preparation. The work on coinjoin privacy mixing protocols will continue as a part of EU HARPA COST project.

CA4_06 Methods for More Compact and Secure Blockchains

- We explored an adaptation of the zkLogin concept for Alphabill. zkLogin eases the access of ordinary users to blockchain-based operations without any need for dedicated key management, as only an already existing relationship with a single sign on (SSO) entity like Google is required to control accounts on Ethereum-like blockchains. We also investigate a trustless design of a 'salt' service with increased abuse–resistance and its practical implementation using the combination of cryptographic hardware, threshold cryptographic protocols for decryption, signing and key derivation.
- Status: Ongoing
- Sustainability: The first part of mini-project is completed, the second one to be finished, released as an open-source during the project duration and published in research publication. The Pressto robot for testing cryptographic devices will be further extended as a part of EU CCAT project.

CA4_07 Blockchain-based intelligent infrastructures

- The core focus of research on blockchain-based intelligent infrastructures is to redesign critical systems to be more secure, transparent, and decentralised. By using blockchain's immutable ledger and cryptographic principles, these infrastructures move away from vulnerable, centralised points of control. For instance, this approach can create forensic ready systems where every access attempt and data transaction is recorded permanently and in a tamper-proof manner, making audits and incident investigations irrefutable. Similarly, in complex environments like the Internet of Vehicles (IoV), blockchain can secure data sharing by combining with Federated Learning. Here, vehicles collaboratively train AI models without sharing raw data, while the blockchain verifies and logs all participant contributions, preventing data poisoning and ensuring trust among untrusted parties. Ultimately, this paradigm shift aims to build systems that are not only intelligent but also inherently resilient and accountable.
- Status: Ongoing
- Sustainability: This ongoing mini project has already produced some results, based on which we have started writing a research paper. The work will continue after CHESS, and the SECURE-NET project will provide funding to support it until completion.

Challenge Area 5: Post-Quantum Cryptography

CA5_01 Aspects of transition to post-quantum technologies

- The aim of the mini-project is to gain experience in transitioning critical digital infrastructure components to post-quantum cryptography. For that, we have selected several projects from the partner's portfolios and created post-quantum versions of them. These projects include a post-quantum encrypted document exchange solution inspired by the CDOC2 infrastructure, a full stack of Web-eID authentication (including the client key storage based on ESP32 microcontroller platform and a PQ-version of NextCoud), and an initial PQ version of the IVXV electronic voting system.
- Status: Ongoing
- Sustainability: Several of these projects (like PQ CDOC2 and IVXV) are currently in active further development and will make it to production within the next few years. A closely related project (PQ version of UXP secure data exchange platform) and PQ-IVXV will also have their development continued under the QARC project.

CA5_02 Implementation of transition to post-quantum technologies

- We designed and implemented experimental software for testing post-quantum secure channels over long distances, with the aim of establishing a secure channel between Estonia and Czechia. Our software, published as open source, makes use of the CRYSTALS-Kyber algorithm to securely establish an encryption key for VPN-like encrypted channel that is realised through Linux-based gateways. This mini-project ended with the publication of the software while work related to the project continues under mini-project CA5_03 on piloting the encrypted post-quantum channel.
- Status: Completed

CA5_03 (Post-)Quantum Communication Infrastructure Pilot

- The objective of this mini-project is to evaluate the software developed in CA5_02 and establish a fully functional quantum-safe communication channel between Czechia and Estonia. We set up a post-quantum virtual private network (VPN) between Estonia and South Moravia to test out the state of the current technology and identify transition challenges. Subsequently, a similar pilot is deployed using hardware devices based on Field Programmable Gate Arrays (FPGAs). The results from piloting are used to further optimise and debug the results.
- Status: Ongoing
- Sustainability: The development and optimisation of post-quantum network traffic encryptors is an ongoing activity and will continue in the QARC project with both Czech and Estonian partners.

Challenge Area 6: Human-centric Aspects of Cybersecurity

CA6_01 Hands-on Cybersecurity Training

- Human-centric cybersecurity relies on the skills and awareness of both professionals and end-users. As a part of this mini-project, we prepared multiple cybersecurity training events for students and educators (trainers) using the KYPO cyber range

platform (an open-source interactive learning environment available at https://crp.kypo.muni.cz/).
- Status: Completed

CA6_02 Improving the usability of penetration testing reports
- This mini-project focuses on penetration testing and ways of improving the reporting process. The effectiveness of penetration testing relies on clear and actionable reporting. A critical challenge lies in ensuring that customers receive informative, easy-to-understand reports. Our aim is to understand the usability gaps in penetration testing reports that can then reveal new methods of writing these reports to help IT professionals, ranging from technical staff to managers, to better implement security measures.
- Status: Ongoing
- Sustainability: This work is ongoing, and will be carried out after the end of CHESS project, attracting interest of senior researchers from University of Arizona (US) and Herriot-Watt University (UK)

CA6_03 Delivering Tabletop Exercises
- This mini-project focuses on the design, delivery, and assessment of tabletop exercises (TTX), with a particular emphasis on the use of the INJECT Exercise Platform – https://inject.muni.cz. Building on the experience of project partners in developing and organizing TTX, the project explores innovative ways to evolve the tabletop exercise format.
- Status: Ongoing
- Sustainability: This work is ongoing and will continue after the completion of the CHESS project, led by MUNI in coordination with NÚKIB, BUT, RIA, UTARTU, and TalTech. The activities will also be supported by the Czech national project CYBER-EDU (VL01010014).

Annex 2

This Annex includes the list of key tools, pilots, methods, and demonstrators.

CA1: Internet of Secure Things

Forensic-Ready Analysis Suite (FREAS) is a tool that facilitates the design of forensic-ready software systems. Such systems integrate proactive preparation for a possible investigation of a security incident or accident in their design. The tool was showcased at the International Conference on Research Challenges in Information Science (RCIS 2024).
Demonstrator URL: https://youtu.be/Y38zS_6XY-I?si=fNT2yQqm2W2-5-f5

The extended version of the libgroupsig library for group signatures. In CA1, we added novel group signature scheme KSAP23. The library with his scheme can be used in complex privacy-preserving solutions, the open-source is available here: https://gitlab.com/brno-axe/chess/extended-gs-lib

CA2: Security Certification

sec-certs system for analyses of the product security certification documents and vulnerabilities. Tool showcased at several world certification conferences, such as the 2024 and 2026 EU Cyber Acts Conferences, 2024 Common Criteria Conference (booth and demonstration organized by Red Hat) or 2024 International Cryptographic Module Conference (with co-funding from the OpenSSL Foundation).

MASS is a tool for evaluating the maturity of an organisation's information security management. The evaluation is based on the Estonian Information Security Standard (E-ITS https://eits.ria.ee), ENISA 2022 Threat Landscape Report (DOI: 10.2824/764318) recommendations and covers ISO27002:2022 control objectives. After evaluating all statements, the respondent will receive an immediate overview of the information security management system situation of their organisation as a downloadable file and as a visual graph. The graph contains ten information security management dimensions that can be used for further planning of the organisation’s information security management. https://mass.cloud.ut.ee/massui/#/

CA3: Verification of Trustworthy Software

Teams in Challenge Area 3 concentrate on developing tools for technology transfer. Their goal is to extend and improve the DiffKemp tool that aims at checking preservation of the semantics of low-level code during refactoring or to improve the efficiency of Perun, a lightweight performance version system as well as a tool suite that helps developers keep the resource consumption of their projects in check throughout the development.

CA4: Security Preservation in Blockchain

The fl-chain-data sharing tool (https://github.com/luzanikita/fl-chain-data-sharing) supports secure data sharing on the Internet of Vehicles using blockchain-based federated learning. The tool is built as a part of master thesis supervised under CA4. The research paper of this tool is currently in progress.

IoV-TwinChain (https://github.com/mubashar-iqbal/vehicle-predictive-maintenance) published in Elsevier Internet of Things journal, the tool performs secure predictive maintenance of vehicles within Internet of Vehicles settings. The tool uses blockchain and digital twin technologies.

DecepSEC tool (https://github.com/mubashar-iqbal/DecepSEC) integrates digital twin and blockchain to enhance the security of Water cyber-physical systems. The research paper of this tool is currently in review phase in the PeerJ computer science journal.

IoTSimulation (https://github.com/mubashar-iqbal/IoTSimulation) tool is built during the master thesis supervised within CA4. The tool support scalability benchmarking of Ethereum blockchain-based IoT applications. The paper on this tool is currently in progress.

An extension of the X-Road, an existing worldwide used data exchange layer, with transparent support for threshold cryptography signatures (RSA, ECDSA), including support for cryptographic hardware https://github.com/crocs-muni/xroad-threshold-signatures presented at the CAISE conference and to X-Road users forums.

Coinjoin privacy mixing analyses (https://crocs-muni.github.io/coinjoin/) were presented at several conferences, including ESORICS'26 and PETS'26, and provide most-extensive public and daily updated insight into the coinjoin ecosystem.

The first practical threshold cryptography support using cryptographic smartcards for anonymous electronic cash of the Cashu system with BDHKE and dBDHKE protocols on the secp256k1 curve https://github.com/crocs-muni/JCMint.

CA5: Post-quantum Cryptography

CA5 produced multiple demonstrators, software implementations and pilots.

- Post-Quantum Cryptography (PQC) in virtual private networks (VPN): a secure communication channel software has been developed, deployed and tested by CHESS consortium partners. The implementation, which is open-source, may be used for larger projects and solutions in PQC: https://gitlab.com/brno-axe/chess/Linux-network-traffic-encryptor
- Hardware-based implementations of post-quantum encryptors were piloted and optimised by CHESS partners. The results of Czech-Estonian pilot led to significant updates of device firmware and reliability improvements. After CHESS, these results will be maintained by the QARC project.
- The PQC VPN solutions were deployed and tested between Brno (Czechia, academia) and Tartu (Estonia, industry).
- The first PQ-enabled document encryption version of the CDOC2 solution.

- The first PQ-enabled version of the IVXV Internet voting system.
- Full-stack PQ authentication solution, including the client key management device based on the ESP32 microcontroller.
- “Post-Quantum Trails” – a board game about post-quantum transition.
- The experience gained during the PoC PQC implementations has found its way to Estonian post-quantum transition roadmap.

CA6: Human-centric Aspects of Cybersecurity

The proof-of-concept implementations, documented in the defended theses of CA6, have been further developed and are now actively used in production to deliver hands-on cybersecurity courses and training. The key components include:

- Hands-on training infrastructure: cross-platform (x86_64, arm64), resource-efficient, and container-based using Docker and Podman;
- Cheating prevention and detection: automated problem generation and detailed logging;
- Class delivery: comprehensive training definitions and materials, incorporating both linear and adaptive hands-on training as well as tabletop exercises.