CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

D1.2 Strategy 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	D1.2
Deliverable name	Strategy for Cross-Regional Collaboration in Cybersecurity
Lead Beneficiary	RIA
Type	R – Document, report
Dissemination Level	PU – Public
Work Package No	WP1
Date	20 December 2024
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.

Editors

- Hendrik Pillmann (RIA)
- 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)
- Alo Lilles (Guardtime)

Reviewers

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

CHESS Consortium

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

Abbreviations

CA - Challenge Area
CHESS - Cyber-security Excellence Hub in Estonia and South Moravia
IoT - Internet of Things
EU - European Union
PQC - Post-Quantum Cryptography
CA - Challange Area
ICT - Information and Communications
SME - Small and Medium Enterprises
IoST - Internet of Secured Things
VPN - Virtual Private Network

Table of Contents

1 Strategic Framework for CHESS

The Cyber Excellence Hub in Estonia and South Moravia (CHESS) is a collaborative initiative uniting leading academic institutions, industry stakeholders, government bodies, and civil society to tackle European most critical cybersecurity challenges. By integrating research, innovation, and practical applications, CHESS aims to strengthen regional and European cybersecurity resilience.

CHESS focuses on six critical Challenge Areas (CAs):

1. Internet of Secure Things (CA1): Securing IoT ecosystems;
2. Security Certification (CA2): Modernizing certification frameworks;
3. Verification of Trustworthy Software (CA3): Enhancing software reliability;
4. Security Preservation in Blockchain (CA4): Scaling secure blockchain applications;
5. Post-Quantum Cryptography (CA5): Preparing for quantum-era threats;
6. Human-Centric Aspects of Cybersecurity (CA6): Focusing on usability and human factors.

In an era of accelerating digital transformation, Europe faces a growing array of cybersecurity threats, from vulnerabilities in interconnected systems to risks posed by emerging technologies like quantum computing. CHESS provides a cohesive framework to address these challenges by bridging the gap between research and real-world application, fostering cross-border collaboration between Estonia and South Moravia – two regions with complementary strengths in cybersecurity – and aligning with EU strategies such as the Cybersecurity Strategy for the Digital Decade and the Digital Compass, ensuring European technological sovereignty and resilience. CHESS matters because it tackles not only today's cybersecurity issues but also anticipates future threats, ensuring European digital ecosystem remains secure and trustworthy.

CHESS is delivering impactful innovations through its focus on tools, pilots, capacity building, and policy alignment. It has developed cutting-edge tools such as the PQC (post-quantum cryptographic) library, the *sec-certs* toolset, and blockchain security solutions, all designed to safeguard critical systems. The initiative has also demonstrated the practicality of its solutions through cross-sector pilot projects in IoT and blockchain, addressing challenges in smart transportation, teleoperation, and critical infrastructure. Furthermore, CHESS addresses skill gaps with tailored training programs and tabletop exercises, enabling participants across public, academic, and industry sectors to tackle cybersecurity challenges effectively. Additionally, the initiative contributes to EU cybersecurity priorities, including post-quantum readiness, IoT certification, and blockchain scalability, while fostering strengthened regional collaboration between Estonia and South Moravia. Together, these efforts form a replicable model for cross-regional cybersecurity excellence.

The CHESS collaborative project is built on the recognition that cybersecurity challenges require cohesive, cross-regional collaboration to drive meaningful innovation, education, and practical solutions. To achieve this, the strategy integrates shared goals that span across all six CAs, fostering collaboration, building capacity, and promoting innovation. These aims not only strengthen the partnership between Estonia and South Moravia but also establish a replicable framework for cybersecurity excellence in other regions.

Central to this strategy is the effort to create meaningful and actionable synergies across Challenge Areas, focusing on realistic collaborations rather than forcing artificial connections. Estonia and South Moravia bring complementary strengths to the table, with Estonian advanced digital government and cybersecurity infrastructure and South Moravian vibrant ICT industry and academic expertise. By connecting these ecosystems, CHESS aims to develop a robust network of stakeholders (including academia, industry, government, and civil society) ensuring sustainable collaboration through shared resources, streamlined governance structures, and practical initiatives such as cross-CA mini-projects and joint knowledge-sharing platforms.

Engaging private companies and public stakeholders is a cornerstone of this effort. These partnerships ensure that research outputs are directly aligned with real-world needs, increasing the likelihood of adoption and economic impact. CHESS prioritizes public-private collaboration by showcasing the tangible benefits of innovative cybersecurity solutions, creating long-term value for both industry and the broader community. Such partnerships align with European and national cybersecurity goals, including those outlined in the EU Cybersecurity Strategy and H2020 flagship initiatives.

Education also plays a pivotal role in CHESS crosscutting aims. The project addresses the critical skills gap by offering tailored training programs, cross-border initiatives, and sector-specific educational content. By targeting skill development in areas such as post-quantum cryptography, IoT security, and blockchain, CHESS ensures that its initiatives prepare professionals to meet evolving challenges. These programs emphasize inclusivity, diversity, and awareness, fostering a workforce capable of driving European digital resilience.

Innovation remains central to bridging the gap between research and practical application. CHESS transforms research into scalable, actionable solutions through small-scale pilots, which serve as proof-of-concept demonstrations for industry and public sector adoption. Dedicated technology transfer efforts, such as brokerage events and technology demonstration days, ensure that innovations reach the market. Startups and SMEs are particularly encouraged to commercialize CHESS-driven technologies, creating a thriving cybersecurity ecosystem.

To sustain these efforts, CHESS leverages local and regional resources, ensuring that its impact extends beyond the project lifecycle. By creating replicable frameworks for innovation, CHESS sets a precedent for other regions, advancing European collective

cybersecurity resilience. These crosscutting aims of collaboration, education, and innovation provide a solid foundation for the project's deep and far-reaching impact.

CHESS is focused on several key steps to ensure its long-term success and impact. Finalizing Action Plans is a priority, with detailed initiatives for each CA, including specific timelines, milestones, and responsibilities to guide implementation. Expanding pilots is essential, particularly in IoT, blockchain, and PQC domains, where successful prototypes can be scaled to address broader, real-world applications. Industry engagement is also critical, requiring strengthened partnerships with private sector stakeholders to promote the adoption of CHESS outputs. A unified training program is under development, aimed at launching cross-CA curricula that address key topics such as post-quantum cryptography and IoT security. Lastly, sustainability planning is a cornerstone of CHESS vision, with efforts to establish a permanent Cybersecurity Excellence Hub as a cross-regional entity that will ensure long-term impact and collaboration.

By advancing these goals, CHESS will not only drive innovation in cybersecurity but also ensure its solutions are scalable, sustainable, and aligned with the needs of European citizens, industries, and governments.

2 Methodology

The CHESS strategy was developed through a collaborative process designed to reflect the strengths, needs, and visions of key stakeholders. By integrating insights from CA leaders and co-leaders, reviewing critical policy documents, and fostering stakeholder engagement, the strategy aligns with regional and European cybersecurity priorities while addressing pressing challenges and opportunities. To achieve this, the development process followed several key steps:

1. **Stakeholder Engagement**

Central to the strategy was engaging with leaders and co-leaders of the six CAs. Semi-structured interviews provided in-depth insights into ongoing research, challenges, and visions for each priority area. This engagement ensured that the strategy captured the perspectives of key contributors and highlighted synergies across CAs. The quadruple helix model, encompassing academia, industry, government, and civil society, guided the inclusion of diverse perspectives.

2. **Data Collection and Analysis**

- **Interviews**: Conducted with CA leaders and co-leaders to understand specific challenges, barriers, and opportunities across the six CAs.

- **Document Review**: Analyzed national and EU cybersecurity strategies, including Estonian and South Moravian smart specialization strategies and the EU Horizon 2020 flagship projects (CONCORDIA, SPARTA, CyberSec4Europe, and ECHO).
- **Benchmarking**: Reviewed best practices from similar cross-regional cybersecurity collaborations to identify scalable and replicable approaches.

3. **Integration and Synthesis**

Findings from interviews and document reviews were synthesized to form a cohesive strategy. This included defining crosscutting aims that integrate the six CAs into a unified framework and designing targeted implementation plans that reflect local and EU priorities.

4. **Iterative Refinement**

Feedback loops were incorporated to ensure the strategy remained dynamic and responsive to emerging needs. Stakeholders were engaged at multiple stages to refine objectives, validate findings, and strengthen alignment with shared goals.

The CHESS strategy is built on a structured methodology designed to ensure inclusivity and an evidence-driven approach. Inclusivity is achieved by actively engaging CA leaders and co-leaders, incorporating diverse perspectives into the strategy. The strategy's foundation is strengthened through structured interviews, comprehensive document reviews, and benchmarking, ensuring thoroughness and reliability. Finally, its relevance is guaranteed by aligning it with EU and national priorities, reinforcing its contribution to broader cybersecurity objectives.

By following this approach, the CHESS strategy delivers:

- A comprehensive understanding of cybersecurity challenges and opportunities in Estonia and South Moravia;
- Six interconnected strategies addressing critical areas, supported by crosscutting aims;
- Practical and actionable plans that bridge the gap between research and real-world applications.

3 Strategies for the Six Challenge Areas

As mentioned before, the CHESS strategy is structured around six interconnected CAs, each addressing critical aspects of cybersecurity. These areas have been carefully selected to respond to both current and emerging threats in the digital landscape, ensuring the initiative relevance and long-term impact. While each CA has distinct priorities, they are

deeply interlinked, providing opportunities for synergies and collaboration that amplify the collective impact of CHESS.

The six CAs serve as the foundation for CHESS research, innovation, and training activities. Each area addresses specific challenges and to ensure the strategies for these areas are effective and actionable, CHESS engaged leaders and co-leaders from each CA through a structured process of interviews and document analysis. This collaborative effort allowed for the creation of focused mini-strategies tailored to the goals, challenges, and practical needs of each area. While these strategies are designed to operate independently, they also align with CHESS overarching goals, fostering collaboration, driving innovation, and addressing critical skills gaps in cybersecurity.

The following sections detail the strategies for each CA, highlighting their unique contributions, alignment with broader cybersecurity priorities, and opportunities for collaboration. Together, they form a cohesive framework for advancing a secure and resilient digital future.

3.1 Internet of Secure Things (CA1)

The Internet of Secure Things (IoST) addresses one of the most critical challenges in cybersecurity: ensuring the security and privacy of interconnected devices in real-world applications. As IoT technologies expand into areas such as smart transportation, teleoperation, and automated systems, their vulnerabilities expose users to significant privacy risks and security threats. CA1 is dedicated to developing scalable, privacy-aware solutions that enhance security across diverse IoT ecosystems, while fostering meaningful collaboration between academia and industry stakeholders.

The core objective of CA1 is to establish frameworks that secure IoT systems and build user trust by prioritizing privacy. This includes conducting research to assess the state of IoT security, identifying gaps, and piloting solutions in domains such as vehicle sharing, teleoperation, and automated systems. These pilots serve as test-environments for validating the practicality and scalability of the developed frameworks and technologies.

Despite its potential, the IoST domain faces notable challenges. Industry engagement remains limited due to a lack of clear financial incentives or demonstrated operational benefits. Bridging the gap between foundational research and practical implementation requires stronger partnerships with private sector stakeholders. Additionally, the competitive IT job market in Estonia and South Moravia makes it challenging to attract young researchers and PhD students. The diversity of IoT applications further complicates the creation of standardized frameworks that can adapt across domains with varying security and privacy requirements.

To overcome these obstacles, CA1 is actively engaging industry partners by showcasing the business value of secure IoT solutions. Tailored use cases and pilot projects demonstrate real-world benefits, encouraging companies to adopt these solutions. Brokerage events and workshops connect researchers with stakeholders, fostering collaborative efforts that deliver mutual value. CA1 also focuses on developing modular, privacy-preserving frameworks that can scale across different IoT applications, enhancing trust and usability.

Education and training are integral to this strategy. CA1 is developing specialized IoT security programs to equip young researchers and professionals with critical skills. Collaborative initiatives between universities and industry partners, such as academic-industry PhD programs, tackle real-world challenges while ensuring a steady pipeline of talent to sustain innovation in IoT security.

Pilot projects are central to CA1 efforts. The focus on smart transportation, including vehicle sharing and teleoperation, highlights the practical applications of IoT security. Partnerships in these areas provide insights that refine the frameworks and ensure their effectiveness in real-world scenarios. These pilots also pave the way for further advancements in automated systems.

Collaboration is a hallmark of CA1, with synergies extending to other CAs. For instance, integrating quantum-safe algorithms from CA5 (PQC) enhances IoT device security, while leveraging user-centric approaches from CA6 (Human-Centric Cybersecurity) improves privacy and usability. Close collaboration with CA2 (Security Certification) supports the development of IoT-specific certification frameworks, fostering trust and compliance across stakeholders.

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, ensuring that IoT security frameworks address both technical and user-centered requirements.

As you can see, CA1 bridges the gap between research and practical implementation, creating secure, privacy-aware IoT ecosystems that address real-world challenges. By combining innovative frameworks, strong industry collaboration, and a focus on education, CA1 establishes a foundation for a safer, more secure IoT.

Key Findings for CA1:

Achievements:

- Developed privacy-aware IoT security frameworks validated through pilot projects in smart transportation and teleoperation systems;
- Progressed foundational research into practical applications, building trust in IoT security solutions;

- Established initial collaborations with industry and academic partners to address real-world IoT challenges.

Challenges:

- 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.

Next Steps:

- Expand industry partnerships by demonstrating the business value of secure IoT frameworks through tailored use cases;
- Scale pilot projects to broader domains, including automated systems, while refining privacy-preserving technologies;
- Develop specialized education programs to attract young researchers and equip professionals with IoT security expertise.

3.2 Security Certification (CA2)

Security certification serves as a cornerstone of trust in cybersecurity systems, ensuring that digital products and services meet rigorous security standards. However, with the growing complexity of digital infrastructures and evolving threats, traditional certification processes must adapt to remain effective, scalable, and transparent. CA2 is focused on modernizing these processes through innovative tools, strategic advocacy, and collaboration.

CA2 is focusing on three key projects: *sec-certs*, F4SLE, and the development of a Common Criteria Security Target for secure multi-party devices. ***sec-certs*** enhances transparency in certification by mapping vulnerabilities and dependencies within certified products, providing users with actionable insights on associated risks. **F4SLE** evaluates organizational security maturity across multiple dimensions, helping institutions assess and improve their security posture. The **Common Criteria Security Target** initiative designs forward-looking frameworks tailored to devices managing shared secrets and cryptographic operations. Collectively, these projects aim to address gaps in current certification systems and promote automated, efficient, and comprehensive approaches.

CA2 faces several challenges. Resistance to updating established certification frameworks, such as Common Criteria, creates barriers to innovation. Limited engagement with key decision-makers, including those at under-resourced organizations like NIST, further complicates progress. Additionally, the labor-intensive nature of certification processes hampers their ability to respond swiftly to emerging threats. Addressing these issues requires a mix of technical advancements, advocacy, and stakeholder collaboration.

To overcome these barriers, CA2 prioritizes refining and scaling its tools and methodologies. The *sec-certs* tool will automate the correlation of certification documents with vulnerabilities, simplifying risk assessments. Advocacy efforts will target leading organizations such as ENISA, BSI, and ANSSI, pushing for the integration of vulnerability mapping into certification frameworks. F4SLE will be expanded into new regions, with translations and pilot implementations showcasing its value to supervisory authorities like NUKIB in the Czech Republic. The Common Criteria Security Target, developed with Cybernetica, will extend beyond government use cases to address broader industry needs.

Collaboration is central to CA2 success. Partnerships with institutions such as Cybernetica and Masaryk University have been pivotal, while synergies with other CAs amplify its impact. For example, CA1 benefits from tailored certification frameworks for interconnected devices, and CA5 ensures quantum-resistant technologies are incorporated into certification processes. CA6 contributes to keeping tools accessible and user-friendly, fostering adoption among diverse stakeholders.

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.

By addressing the limitations of traditional frameworks, CA2 is transforming security certification into a transparent, automated, and adaptable process. Its efforts not only build trust in cybersecurity systems but also lay the groundwork for a more resilient digital ecosystem.

Key Findings for CA2:

Achievements:

- Developed tools like *sec-certs* to map vulnerabilities and dependencies in certification processes, improving transparency and risk assessment;
- Launched F4SLE to evaluate organizational security maturity and support institutions in strengthening their security posture;
- Initiated the creation of a Common Criteria Security Target to future-proof certification for secure multi-party devices.

Challenges:

- Resistance to modifying well-established certification frameworks, such as Common Criteria;
- Limited engagement with decision-makers at key organizations like NIST due to resource constraints;
- Labor-intensive certification processes limit responsiveness to rapidly evolving threats.

Next Steps:

- Enhance the *sec-certs* tool by automating its correlation of certification documents with vulnerabilities, facilitating broader adoption;
- Advocate for integrating vulnerability mapping into certification frameworks through engagement with ENISA, BSI, ANSSI, and the European Commission;
- Expand F4SLE to additional regions through translations and pilot implementations to demonstrate its value to supervisory authorities and organizations;
- Strengthen collaboration with other CAs, such as CA1, to develop certification frameworks tailored to interconnected devices.

3.3 Verification of Trustworthy Software (CA3)

Ensuring the reliability and security of software systems is a cornerstone of modern cybersecurity. CA3 advances methods for software verification, addressing the increasing complexity of digital systems while bridging the gap between foundational research and real-world application. By developing tools and techniques that enhance trustworthiness, CA3 targets critical challenges in software security through three main research streams.

The first stream focuses on applying program analysis techniques to practical software development, emphasizing tools that facilitate technology transfer between academia and industry. A key achievement in this area is ***Symbiotic***, a program analysis tool designed to identify vulnerabilities and optimize software performance. Collaboration with industry partners, such as Red Hat, has been instrumental in refining and adopting Symbiotic functionalities.

The second stream explores cryptographic protocols, developing theoretical and practical approaches to improve their robustness and identify limitations. This includes compositional techniques for understanding and verifying cryptographic systems. The third stream addresses emerging challenges in formal methods, particularly the synthesis of efficient and safe software controllers for multi-agent systems operating in complex environments.

While CA3 has made significant strides, several challenges persist. A shortage of skilled professionals, especially young researchers and PhD students, poses a barrier to sustaining advancements in formal methods and software verification. Industry adoption of tools like Symbiotic remains limited due to the need for clearer evidence of their practical value. Additionally, the highly technical nature of this work requires better communication and outreach to ensure its outputs are accessible and applicable to diverse stakeholders.

To address these challenges, CA3 focuses on expanding tool adoption and strengthening industry collaboration. This includes refining tools like Symbiotic and creating clear, practical use cases that demonstrate their value. Initiatives such as **Industrial Days** bring together researchers and industry practitioners to foster knowledge exchange and explore opportunities for technology transfer. These events provide a platform for showcasing CA3

tools and fostering partnerships with companies that can implement them in real-world scenarios.

Education and training are integral to CA3 strategy. Specialized workshops and training programs on software verification aim to attract and retain talent while equipping professionals with the skills to address emerging challenges. Collaboration with academic institutions and industry partners ensures these programs balance theoretical foundations with practical applications, creating a pipeline of skilled professionals capable of advancing software security.

Collaboration with other CAs enhances CA3 impact. For example, integrating software verification techniques into certification frameworks (CA2) ensures certified systems meet high trustworthiness standards. Similarly, CA5 provides opportunities to test and verify cryptographic protocols within post-quantum environments, contributing to the security of next-generation systems.

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.

By advancing formal methods and program analysis, CA3 plays a critical role in ensuring the reliability and security of digital systems. Its focus on bridging academic research and industrial application enhances software trustworthiness while laying the foundation for future innovations in cybersecurity.

Key Findings for CA3:

Achievements:

- Developed tools like Symbiotic for program analysis, enabling vulnerability identification and software optimization;
- Collaborated with industry partners, including Red Hat, to refine and implement software verification tools;
- Advanced theoretical work on cybersecurity protocols and formal methods for software controller synthesis.

Challenges:

- Shortage of skilled professionals, particularly young researchers and PhD students, to sustain and expand formal methods research;
- Limited industry adoption of software verification tools due to the need for clearer evidence of their practical value;
- Highly technical outputs require improved communication and outreach for broader usability and adoption.

Next Steps:

- Expand adoption of tools like Symbiotic by developing clear use cases and showcasing practical benefits to industry stakeholders;
- Strengthen industry collaborations through initiatives like Industrial Days to foster knowledge exchange and technology transfer;
- Develop specialized training programs and workshops to attract new talent and equip professionals with verification expertise;
- Integrate software verification techniques into certification frameworks (collaborating with CA2) and test cryptographic protocols within post-quantum environments (collaborating with CA5).

3.4 Security Preservation in Blockchain (CA4)

CA4 explores blockchain dual role as a security enabler while addressing its inherent risks and limitations. Its aim is to create scalable, secure, and practical blockchain applications that support critical systems across various domains. Through targeted research and strategic collaboration, CA4 has achieved notable progress and continues to tackle key challenges.

In 2023, CA4 successfully completed three mini-projects. The first, **Automated Trust through Self-Sovereign Identity**, developed decentralized identity solutions to enhance trust in digital transactions. The second, **Emergency Information Transmission Using Blockchain** demonstrated blockchain capability to secure critical data exchanges in vehicular communication networks. The third, **Blockchain Operations Secured by Cryptographic Hardware**, improved blockchain resilience through advanced cryptographic techniques. Building on these efforts, three new mini-projects launched in 2024. These include **Secure Information Transmission in Intelligent Vehicles**, which safeguards vehicle-to-vehicle and vehicle-to-infrastructure communication; **Privacy of Blockchain Transactions**, employing zero-knowledge proofs to enhance privacy; and **Methods for Compact and Secure Blockchains**, which address scalability and data processing inefficiencies.

Collaboration has been pivotal to CA4 success. Partnerships with the University of Tartu, Masaryk University, and Cybernetica have advanced research and implementation efforts. However, challenges remain, including communication gaps between institutions and alignment of cross-border research interests. The limited size of participating countries further restricts the pool of researchers and industries sharing common objectives. Expanding international collaboration and strengthening engagement with industrial stakeholders remain key priorities.

A major barrier to blockchain adoption in industrial settings is the misconception that blockchain is exclusively tied to cryptocurrency. This association limits exploration of blockchain broader potential. Additionally, regulatory differences and varying levels of industry readiness create further obstacles. Addressing these challenges requires targeted

educational outreach to demystify blockchain and demonstrate its diverse applications beyond financial systems.

CA4 strategic objectives focus on advancing research, fostering industry engagement, and strengthening international collaboration. Research priorities include enhancing privacy through zero-knowledge proofs and optimizing blockchain scalability and security. Industry partnerships are critical for validating solutions in real-world scenarios, particularly in intelligent transportation and critical infrastructure. International collaboration helps build a global network of stakeholders to amplify the adoption and impact of CA4 work.

Synergies with other CAs enhance CA4 outcomes. Collaborations with CA5 focus on integrating quantum-resistant methods to future-proof blockchain systems, while partnerships with CA6 aim to make blockchain solutions more intuitive and user-friendly.

CA4 success will be measured through the adoption of its solutions in pilot projects, the development of innovative tools and research outputs, and the establishment of strong industry partnerships. Metrics such as high-impact publications, stakeholder feedback, and outreach effectiveness will provide insights into the progress and impact of CA4 initiatives.

By addressing blockchain limitations and demonstrating its transformative potential, CA4 positions the technology as a secure and reliable foundation for critical systems. Through targeted research, collaboration, and practical applications, CA4 contributes meaningfully to the broader cybersecurity ecosystem.

Key Findings for CA4:

Achievements:

- Successfully completed three mini-projects in 2023, including decentralized identity solutions, blockchain-secured vehicular communication, and cryptographic hardware protection for blockchain operations;
- Initiated three new mini-projects in 2024, focusing on secure information transmission in intelligent vehicles, privacy enhancements for blockchain transactions, and methods for compact and secure blockchains;
- Strengthened collaborations with the University of Tartu, Masaryk University, and Cybernetica to advance blockchain research and applications.

Challenges:

- Misconceptions about blockchain being tied exclusively to cryptocurrency hinder broader industrial adoption;
- Communication gaps between institutions and national stakeholders limit the potential of cross-border collaboration;
- Regulatory differences and varying levels of industry readiness create barriers to implementation.

Next Steps:

- Address misconceptions through targeted outreach and education to showcase blockchain applications beyond cryptocurrency;
- Enhance privacy features in blockchain systems using techniques like zero-knowledge proofs.
- Scale pilot projects for blockchain-based solutions in intelligent transportation and critical infrastructure sectors;
- Collaborate with CA5 to integrate quantum-resistant cryptographic methods into blockchain protocols and with CA6 to improve accessibility and usability of blockchain solutions for end-users.

3.5 Post-Quantum Cryptography (CA5)

The advent of quantum computing presents both opportunities and existential threats to existing cryptographic systems. Post-Quantum Cryptography (PQC) addresses this challenge by developing quantum-resistant solutions to secure digital infrastructures in the quantum era. CA5 focuses on creating and testing practical implementations of these algorithms across diverse use cases, ensuring a resilient transition to quantum-safe systems.

CA5 work is anchored in several key projects, including use cases for authentication, encryption, Virtual Private Networks (VPNs), and the large-scale task of transitioning entire infrastructures, exemplified by the “Evil Twin” use case. Central to these efforts is the development of a **PQC library**, a modular and scalable software module that integrates quantum-resistant functionality across applications. This library is designed for flexibility, enabling seamless integration into future systems.

CA5 faces unique challenges. The shortage of cryptographic expertise among researchers and implementers creates bottlenecks for developing and deploying post-quantum systems. Foundational research projects, such as those addressing voting infrastructure, remain in early stages, requiring significant development before achieving real-world implementation. Additionally, limited awareness among stakeholders about the urgency and practical steps for post-quantum readiness hinders broader adoption.

To address these challenges, CA5 emphasizes collaboration, education, and flexibility. Partnerships with institutions like Brno University of Technology and Cybernetica have driven advancements, including progress on the VPN use case, which has already resulted in open-source software and publications. Broader cryptographic education is a priority, focusing on building a skilled workforce and equipping governments and organizations to procure and manage post-quantum systems effectively. Incremental transitions are a key strategic approach, allowing individual components to be secured before scaling to broader infrastructures. This ensures measurable progress while adapting to rapidly evolving quantum technologies.

Synergies with other CAs enhance CA5 contributions. Integrating PQC algorithms into IoT systems (CA1) enhances their resilience against quantum threats, while collaboration with CA2 ensures post-quantum standards are incorporated into certification frameworks, fostering trust and compliance. These collaborations underscore the cross-disciplinary nature of post-quantum efforts and their critical role within the broader cybersecurity ecosystem.

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.

In conclusion, CA5 plays a pivotal role in preparing digital infrastructures for the quantum era. By focusing on collaboration, education, and incremental implementation, CA5 ensures that cybersecurity systems remain resilient against emerging threats posed by quantum computing, contributing to a secure and future-proof digital landscape.

Key Findings for CA5:

Achievements:

- Created a modular and scalable PQC library for diverse use cases, including authentication, encryption, and VPNs;
- Initiated pilot implementations to transition infrastructures to quantum-safe algorithms, including the “Evil Twin” use case for large-scale systems;
- Developed open-source software for PQC-secure channel demonstration and evaluation;
- Published research on quantum-resistant cryptographic methods in collaboration with academic and industrial partners, such as Brno University of Technology and Cybernetica.

Challenges:

- Shortage of expertise in cryptography, particularly in the development and deployment of post-quantum systems;
- Foundational research projects require significant development before transitioning to operational systems;
- Limited awareness and understanding among stakeholders about the urgency and practical steps needed for post-quantum readiness.

Next Steps:

- Expand pilot implementations of the PQC library to test and refine quantum-resistant cryptographic algorithms across diverse environments;
- Develop training programs and educational materials to address the skills shortage and equip organizations to implement post-quantum systems effectively;

- Incrementally transition critical infrastructure components to quantum-safe algorithms, focusing on securing individual systems before scaling;
- Collaborate with CA1 to integrate quantum-safe protocols into IoT systems and with CA2 to align certification frameworks with post-quantum standards;
- Organize awareness-raising events across all sectors of the quadruple helix to foster connections and support the transition to PQC.

3.6 Human-Centric Aspects of Cybersecurity (CA6)

Cybersecurity is not just a technical challenge – it is deeply intertwined with human behavior, decision-making, and the usability of tools and systems. CA6 focuses on designing security solutions that are accessible, intuitive, and aligned with the needs of end-users. By prioritizing the human element, CA6 addresses gaps in awareness, training, and usability, fostering a holistic approach to cybersecurity.

CA6 work spans training and education, usability testing, and stakeholder engagement. A key focus is on developing **tabletop exercises** and practical training programs to equip diverse audiences (from IT professionals and public sector employees to non-technical users) with the skills to navigate complex cybersecurity challenges. These initiatives ensure cybersecurity knowledge is widely disseminated and actionable.

One of CA6 central challenges is bridging the gap between technical security measures and their adoption by end-users. Many tools prioritize technical efficacy but overlook usability, leading to resistance or improper implementation. Building a culture of cybersecurity awareness also requires sustained effort, especially in regions where cybersecurity is not a top priority. Limited resources for large-scale usability studies and training expansion further constrain progress.

To address these challenges, CA6 emphasizes collaboration and education. Partnerships with universities, government agencies, and industry stakeholders enable the development of targeted training programs tailored to specific sectors. Tabletop exercises, simulating real-world cyber incidents, allow participants to practice response strategies and improve preparedness. Usability testing and user feedback further enhance the accessibility and adoption of cybersecurity tools, reducing risks from misconfigurations and errors.

CA6 efforts intersect with other CAs, reinforcing the interconnected nature of cybersecurity. Training and awareness programs complement technical innovations in CA1 and CA4 by ensuring users understand and trust these systems. Collaboration with CA2 bridges the gap between certification processes and practical implementation, making certifications more accessible and user-friendly.

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.

In conclusion, CA6 emphasizes that cybersecurity is as much about people as it is about technology. By focusing on human-centric solutions, it ensures security measures are accessible, effective, and widely adopted. Through training, usability improvements, and stakeholder engagement, CA6 contributes to a cybersecurity ecosystem that is inclusive, resilient, and responsive to the needs of all users.

Key Findings for CA6:

Achievements:

- Developed tailored training programs and tabletop exercises to improve cybersecurity awareness and preparedness among diverse audiences;
- Conducted usability testing to enhance the accessibility and adoption of cybersecurity tools and systems;
- Fostered collaborations with stakeholders to align human-centric approaches with technical innovations in other CAs.

Challenges:

- Bridging the gap between security measures and their adoption by end-users when tools are overly technical or complex;
- Sustaining efforts to build a culture of cybersecurity awareness in regions where it is not a top priority;
- Limited resources for large-scale usability studies and expanding the reach of training programs.

Next Steps:

- Expand training programs and tabletop exercises to target more sectors and user groups, ensuring broader dissemination of cybersecurity knowledge;
- Strengthen usability testing to refine cybersecurity tools, ensuring they balance technical requirements with user needs;
- Collaborate with CA1 and CA4 to build user trust and understanding of new systems and tools;
- Bridge the gap between certification frameworks (CA2) and practical implementation by making certification processes more accessible and user-friendly.

4 Integration of Strategies

The six CAs within CHESS are interconnected pillars of a unified cybersecurity strategy. By identifying realistic synergies and fostering meaningful collaboration, CHESS amplifies the collective impact of its activities, ensuring a cohesive and impactful approach to addressing

cybersecurity challenges. Several cross-cutting themes underscore the interconnected nature of the CAs, including collaboration with industry and stakeholders, education and capacity building, and the need to bridge research with practical applications.

Collaboration with private sector partners and policymakers is essential for translating research into real-world applications. For example, CA1 (IoT Security) and CA4 (Blockchain) depend on industry collaboration for pilot implementations, while CA2 (Security Certification) focuses on aligning certification frameworks with stakeholder needs. Meanwhile, training and workforce development are central across CAs, particularly in CA3 (Verification of Trustworthy Software), CA5 (PQC), and CA6 (Human-Centric Cybersecurity). A unified strategy ensures these efforts address skill gaps comprehensively across domains. Similarly, bridging research and practice is a shared focus, with CAs like CA2 and CA3 emphasizing the development of practical tools and frameworks that align academic advancements with real-world cybersecurity challenges.

Each CA contributes unique expertise and tools that enhance others. For instance, CA2 *sec-certs* and CA5 PQC Library provide foundational tools that integrate seamlessly into CA1 IoT systems and CA4 blockchain applications. CA6 ensures that technical innovations across other CAs are accessible and intuitive, improving adoption and reducing user errors, while CA5 provides quantum-resistant cryptographic technologies critical for securing IoT devices (CA1) and blockchain systems (CA4).

The success of one CA often supports or depends on another. IoT security frameworks (CA1) rely on robust certification processes (CA2) to build trust and ensure compliance. Blockchain systems (CA4) benefit from integrating quantum-resistant cryptography (CA5) to maintain long-term security. Usable and trustworthy software solutions (CA3) depend on rigorous verification techniques and user-centric designs (CA6).

To maximize collaboration and integration, CHESS emphasizes collaborative pilot projects that involve multiple CAs. For instance, securing IoT systems (CA1) could integrate blockchain for data integrity (CA4), certification frameworks (CA2), and user-focused training (CA6). Unified training programs drawing expertise from all CAs target priority areas such as post-quantum cryptography, blockchain security, and usability in cybersecurity. These initiatives align with stakeholder needs and are delivered through workshops, online modules, and academic partnerships. Cross-CA working groups address shared challenges, such as integrating quantum-safe algorithms (CA5) into IoT systems (CA1) or improving the usability of certification tools (CA2). Clear, shared success metrics, such as adoption rates, stakeholder feedback, and pilot outcomes, provide a consistent framework for evaluating integration effectiveness, supported by regular feedback loops to ensure continuous improvement. Targeted advocacy efforts tailored to specific stakeholder groups further enhance visibility and adoption of CHESS outputs.

By fostering meaningful synergies, shared initiatives, and aligned actions, CHESS ensures its collective efforts are more impactful than the sum of individual CAs. This integrated approach creates a robust, interconnected framework for advancing cybersecurity at both regional and European levels.

5 Implementation Roadmap

The CHESS initiative is guided by a clear and actionable roadmap designed to achieve its goals across all six CAs. By integrating timelines, milestones, and a governance framework, the roadmap ensures cohesive progress, prioritizing both immediate objectives and long-term advancements in cybersecurity. By leveraging the interdependencies between CAs, CHESS maximizes its impact, ensuring that progress in one area reinforces advancements in others.

The six CAs form interdependent pillars of CHESS cybersecurity strategy. Their outputs are interconnected, creating synergies that strengthen the initiative. IoT security frameworks (CA1) incorporate quantum-resistant cryptography from CA5 to ensure long-term resilience. Certification tools from CA2, such as *sec-certs*, integrate with software verification techniques from CA3 to enhance trustworthiness. Blockchain systems (CA4) utilize post-quantum algorithms from CA5 to future-proof security, while human-centric solutions (CA6) improve the usability and adoption of tools and frameworks developed across other CAs, ensuring stakeholder engagement and reducing barriers to implementation. By fostering these synergies, CHESS creates a robust framework where advancements in one CA amplify progress across others.

The roadmap progresses through four distinct phases, ensuring structured and scalable activities across all CAs:

1. **Foundations**: The initial phase focuses on establishing research collaborations and developing tools, frameworks, and strategies ready for pilot testing. Prototypes such as *sec-certs* and the PQC library are completed, along with pilot implementation plans. This phase is designed for completion within the first year.

2. **Pilots**: The second phase involves implementing pilot projects to validate tools and frameworks, accompanied by tabletop exercises and usability studies to gather valuable feedback from end-users. Deliverables include validated tools, training programs, and comprehensive reports on pilot outcomes. This phase unfolds over the second and third years.

3. **Scaling**: During this phase, pilot implementations are expanded to include additional domains and stakeholders, fostering stronger collaborations with industry and international partners. Solutions are scaled for deployment across diverse sectors and regions. This phase is scheduled for the third and fourth years.

4. **Sustainability**: The final phase transitions tools and frameworks into operational use, supported by long-term governance structures and funding mechanisms. Deliverables include fully operational tools, established partnerships, and sustainability strategies to ensure continued impact. This phase begins in the fifth year and extends beyond the project timeline.

A robust governance framework underpins the roadmap effective implementation. A Strategy Board, comprising representatives from all key partners, oversees progress, resolves

conflicts, and provides strategic guidance. CA Working Groups, led by CA leaders and co-leaders, manage day-to-day operations and submit quarterly progress reports. A Cross-CA Integration Team facilitates synergies through joint initiatives, pilot projects, and shared training programs, while an External Advisory Board of independent experts provides high-level feedback and aligns CHESS efforts with European cybersecurity priorities.

Progress is tracked using predefined metrics for each CA, including adoption rates of developed tools, stakeholder engagement levels, and the impact of pilot projects. Annual reviews ensure the roadmap remains responsive to emerging challenges and opportunities, allowing CHESS to adapt while staying aligned with its strategic goals.

By integrating timelines, milestones, and collaborative governance, CHESS ensures that its activities are impactful, efficient, and sustainable. This roadmap creates a strong foundation for advancing cybersecurity at regional and European levels, fostering long-term growth of the cybersecurity ecosystem.

6 Resources and Sustainability

The long-term success of the CHESS initiative depends on securing the necessary resources to implement its strategies and sustain outcomes beyond the project lifecycle. Shared and CA-specific resources (including technical, financial, and human capital) are critical to maintaining progress and ensuring enduring impact. This section outlines resource needs and sustainability strategies to create lasting value across all six CAs.

CHESS requires a combination of shared resources to achieve its goals and foster cross-CA collaboration. A skilled workforce of researchers, developers, and industry professionals is essential. Targeted recruitment, training, and capacity-building programs are needed to address talent shortages in key areas like cryptography (CA5) and software verification (CA3). Funding from European initiatives (e.g., Horizon Europe, Digital Europe), national programs, and private sector investments will drive the development and scaling of tools, pilot projects, and training programs. Robust hosting environments, shared labs, and testing platforms are necessary to support tools like the PQC library (CA5) and the *sec-certs* tool (CA2). Additionally, a centralized digital platform for knowledge sharing, project management, and tool integration will streamline communication and foster synergies across CAs.

Each CA has unique resource requirements tailored to its specific focus areas and deliverables. CA1 (Internet of Secure Things) requires access to IoT testbeds and pilot environments for smart transportation and automated systems, as well as partnerships with industry to scale solutions. CA2 (Security Certification) needs support for advancing tools like *sec-certs* and F4SLE, alongside advocacy resources for driving certification reform and engaging with certification bodies. CA3 (Verification of Trustworthy Software) demands skilled personnel to enhance tools like Symbiotic and funding for expanded pilot testing in diverse software environments. CA4 (Security Preservation in Blockchain) requires blockchain testing infrastructure, particularly for IoV and critical infrastructure contexts, and collaboration with regulatory bodies. CA5 (PQC) needs funding for large-scale testing of

quantum-resistant algorithms and partnerships with industries to implement these solutions in real-world scenarios. CA6 (Human-Centric Cybersecurity) requires resources for usability studies, the delivery of training programs, and the development of tailored tabletop exercises for diverse user groups.

To ensure CHESS outcomes endure, a multi-faceted sustainability strategy has been developed. A permanent Cybersecurity Excellence Hub supported by Estonia and South Moravia will serve as a central node for ongoing research, collaboration, and innovation. Long-term partnerships with academic institutions, industry leaders, and government agencies will maintain engagement. Leveraging EU programs (Horizon Europe, Digital Europe) will provide continued support for CHESS activities, while public-private partnerships and private sector investments will fund pilot projects, commercialization, and scaling efforts. Advocating for national funding will integrate CHESS outputs into regional and local cybersecurity strategies.

Educational initiatives will expand by embedding training modules from CAs 3 and 6 into university curricula, professional certification programs, and industry workshops. Scholarships and exchange programs will build cybersecurity capacity and address talent shortages. CHESS-developed tools, such as the PQC library and blockchain security frameworks, will transition into scalable products for broader adoption, supported by industry partnerships that establish commercialization pathways.

Aligning CHESS outcomes with European cybersecurity priorities ensures continued relevance and support. Regulatory frameworks that incentivize the adoption of CHESS-developed methodologies, such as quantum-safe cryptography and IoT certification frameworks, will be a key focus. A long-term monitoring framework will track adoption, scalability, and the impact of CHESS outputs. Collaboration levels, user feedback, and the performance of deployed tools will be regularly evaluated to ensure continuous improvement.

Resources and sustainability are central to CHESS ability to drive lasting change in cybersecurity. By addressing shared and CA-specific resource needs and implementing robust strategies, CHESS ensures its innovations and partnerships endure beyond the project lifecycle. This approach strengthens regional cybersecurity capabilities while contributing to European overall digital resilience.

7 Metrics and Evaluation

Evaluating the success of CHESS is critical to ensuring it delivers on its mission to enhance cybersecurity capabilities, foster collaboration, and drive innovation. The evaluation framework captures both overarching achievements and the specific contributions of the six CAs, establishing a foundation for accountability, learning, and continuous improvement. By defining clear metrics and employing robust assessment methods, CHESS ensures its activities are impactful and aligned with its strategic goals.

The metrics framework operates on two levels: overarching goals for CHESS as a whole and tailored objectives for each CA. This dual approach provides a comprehensive understanding of progress, with overarching metrics measuring CHESS collective impact on collaboration, innovation, and education, while CA-specific metrics track progress in pilot projects, tools, and training programs. Detailed metrics and milestones will be outlined in the upcoming Action Plans, focusing on quantifiable outcomes such as tool adoption rates, training participation, and the effectiveness of pilot implementations. This ensures a systematic approach to tracking progress and refining activities.

Each CA's success is assessed through tailored metrics that reflect its unique objectives. For CA1 (Internet of Secure Things), success is measured by the number of IoT pilot projects completed and the adoption rates of IoT security frameworks by industry. For CA2 (Security Certification), metrics include the adoption rates of tools like *sec-certs* and F4SLE, and progress in reforming certification frameworks. CA3 (Verification of Trustworthy Software) focuses on the number of software verification tools deployed and collaborations established through Industrial Days. CA4 (Security Preservation in Blockchain) tracks the number of blockchain pilot projects completed and the integration of zero-knowledge proofs in industry solutions. For CA5 (), readiness and adoption of quantum-resistant tools and stakeholder feedback on pilot projects are key indicators. Finally, CA6 (Human-Centric Cybersecurity) evaluates the number of participants trained and improvements in usability and adoption of cybersecurity tools.

At the overarching level, CHESS ability to foster collaboration, advance innovation and research, and promote education and capacity building serves as a benchmark for success. Metrics in fostering collaboration include the number of active partnerships across academia, industry, and government, as well as the quality and frequency of knowledge-sharing activities such as workshops and cross-border mobility programs. For advancing innovation, the development and adoption of new tools, frameworks, and methodologies, as well as high-impact publications and follow-up funding success, reflect tangible outcomes of CHESS research activities. Education and capacity building are assessed through the number of individuals trained, the integration of training modules into curricula, and feedback from participants.

CHESS employs a combination of quantitative and qualitative methods to ensure comprehensive evaluation. Quantitative analysis includes adoption rates, publication impact factors, and training completion rates, which provide concrete evidence of progress. Stakeholder surveys and feedback capture insights from participants, partners, and end-users, ensuring the initiative remains relevant and impactful. In-depth case studies of pilot projects and successful collaborations highlight best practices and lessons learned, offering a deeper understanding of effective strategies. To maintain transparency and accountability, annual impact reports synthesize all evaluation data, providing a clear overview of progress aligned with both overarching goals and CA-specific objectives. Quarterly progress reviews from CA leaders track milestones, challenges, and achievements, while regular stakeholder feedback informs continuous improvement.

This metrics and evaluation framework ensures that CHESS strategies are effective, adaptable, and impactful. By combining clear metrics with robust assessment methods, CHESS provides a roadmap for continuous improvement, accountability, and learning. This

framework not only measures success but also ensures CHESS contributions to cybersecurity resilience are meaningful, scalable, and sustainable.

8 Alignment with EU Policies

CHESS is strategically aligned with both European and national cybersecurity policies, ensuring its outputs advance the shared goals of resilience, innovation, and trust in digital systems. By addressing critical cybersecurity challenges through its six CAs, CHESS supports the objectives of the EU Cybersecurity Strategy for the Digital Decade, the Digital Compass, and the Cyber Resilience Act while complementing Estonian and Czech national strategies.

The EU Cybersecurity Strategy for the Digital Decade calls for enhanced resilience, technological sovereignty, and collaboration across member states. CHESS contributes directly to these priorities by developing scalable solutions that secure critical sectors such as IoT (CA1) and blockchain systems (CA4), while advancing PQC (CA5) to prepare for emerging threats. Its collaborative framework, which bridges academia, industry, and government, embodies the multi-stakeholder approach promoted by the EU. By creating tools like *sec-certs* and F4SLE (CA2) to improve certification processes and fostering skills development to address workforce gaps (CA6), CHESS reinforces European position as a global cybersecurity leader.

As outlined in the Digital Compass, European digital transformation depends on secure and sustainable digital infrastructures. CHESS plays a key role by ensuring IoT security frameworks (CA1) protect interconnected devices and systems, providing blockchain-based solutions (CA4) to enhance trust in decentralized technologies, and developing quantum-resistant standards (CA5) to safeguard digital infrastructure from future threats. By embedding cybersecurity training into education systems (CA6), CHESS addresses the skills pillar of the Digital Compass, closing workforce gaps and creating a robust foundation for European digital ambitions.

The Cyber Resilience Act sets out baseline security requirements for digital products and connected devices. CHESS aligns with this regulation by operationalizing security-by-design and lifecycle management principles through pilot projects in IoT (CA1) and certification tools (CA2). These outputs provide practical pathways for compliance, making cybersecurity accessible and achievable for businesses and industries.

CHESS also integrates national cybersecurity strategies from Estonia and Czechia into its work, ensuring regional needs are addressed while contributing to EU-wide goals. In Estonia, CHESS aligns with the Cybersecurity Strategy for 2024–2030, which focuses on resilience, safeguarding critical infrastructure, and fostering awareness. Outputs like IoT security pilots (CA1) and blockchain-based solutions for infrastructure (CA4) resonate with these priorities. The project also supports Estonian RDIE Strategy 2021–2035, driving innovation and economic growth through cybersecurity advancements. In Czechia, CHESS supports the National Cybersecurity Strategy 2021–2025, which emphasizes advanced

research and cross-border collaboration. Initiatives like software verification (CA3) and post-quantum cryptography pilots (CA5) accelerate technological adoption, while collaboration with NUKIB ensures alignment with Czech National Plan for Research and Development in Cybersecurity 2025.

To amplify its impact, CHESS actively engages with existing resources and networks. RIA Yearbooks and Studies provide insights into emerging threats, shaping CHESS initiatives, while NUKIB Reports highlight key areas for integrating CHESS outputs into national frameworks. EU Networks such as ENISA, NCCs, and EDIHs serve as platforms for sharing CHESS outputs across member states and embedding them into EU-wide policies.

By aligning with EU and national priorities, CHESS ensures its outputs are scalable and impactful. Tools like blockchain security solutions (CA4) and quantum-resistant standards (CA5) can shape European certification schemes and regulatory frameworks, while its collaborative model serves as a blueprint for fostering cross-border cybersecurity excellence. Through continued engagement with European and national bodies, CHESS remains a cornerstone of European digital resilience.

9 Conclusions and recommendations

The CHESS initiative has demonstrated that regional collaboration, targeted research, and practical innovation can address pressing cybersecurity challenges while contributing to European broader digital resilience. By uniting Estonia and South Moravia, two regions with complementary strengths in cybersecurity and digital innovation, CHESS has created solutions for today's challenges and laid the groundwork for addressing future threats. Its six CAs provide a comprehensive approach to cybersecurity, combining technical advancements, human-centric design, and cross-disciplinary collaboration. However, for these efforts to achieve their full potential, it is essential to consolidate lessons learned, act on specific recommendations, and ensure sustainability through a strong commitment from all stakeholders.

While this strategy provides a comprehensive vision for advancing cybersecurity, its true impact lies in the concrete steps that will follow. Detailed Action Plans for each Challenge Area will translate strategic goals into specific initiatives. These will address the research, training, and innovation needs identified in Deliverable D1.1, focusing on measurable outcomes through collaborative projects, capacity building, and pilot implementations. The Action Plans will ensure that CHESS achieves its mission of fostering a secure and resilient digital ecosystem.

Moving forward, institutionalizing CHESS outputs is crucial to ensure their long-term impact. Tools, frameworks, and methodologies must be embedded into regional and national cybersecurity strategies while aligning with broader European priorities. The scalability of pilot projects, the integration of post-quantum cryptography standards, and the adoption of IoT security frameworks must be reinforced through collaborative partnerships and regulatory alignment. The journey of CHESS has underscored the need for collaboration,

integrating research with real-world applications, and addressing skill gaps in the cybersecurity workforce. Each CA contributes uniquely to the overall vision, from developing quantum-resistant cryptography to advancing usability in cybersecurity tools. Scaling and institutionalizing these outputs will embed CHESS contributions into European cybersecurity frameworks.

Fostering collaboration is essential for sustained impact. Formalizing the Cybersecurity Excellence Hub model established by CHESS would create a permanent cross-regional platform for research, knowledge-sharing, and practical implementation. This hub would serve as a long-term structure to maintain CHESS momentum and replicate its success across Europe. Strengthened engagement with industry partners is equally critical. Many stakeholders have expressed interest in CHESS tools but require clearer incentives to participate in pilot projects or adopt solutions. Regulatory support, funding mechanisms, and practical demonstration projects will be vital in bridging this gap.

Education and capacity building must remain a priority. Embedding training modules and best practices developed by CHESS into university programs, professional certifications, and workplace training will address the cybersecurity skills shortage. Scholarships and exchange programs can further build capacity and develop a skilled workforce.

Aligning CHESS outputs with European cybersecurity priorities is essential for sustained relevance. Close collaboration with policymakers will ensure tools, standards, and frameworks are integrated into EU-level strategies, such as the Digital Compass and the Cybersecurity Strategy for the Digital Decade. This alignment will enhance the visibility of CHESS contributions and attract further funding and collaboration opportunities.

Each CA's outputs require tailored actions to maximize their impact. 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. Finally, 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.

The active participation of stakeholders across all levels—regional, national, and European—is key to CHESS success. Governments in Estonia and South Moravia must integrate CHESS outputs into their national strategies and support cross-border initiatives. Industry partners, particularly those engaged in pilot projects, should be incentivized to adopt CHESS-developed tools and frameworks, demonstrating their practical value in real-world applications. Academic institutions must sustain CHESS impact by embedding its training modules into curricula and fostering the next generation of cybersecurity professionals. Meanwhile, the European Union should amplify CHESS achievements by funding follow-up projects, adopting its standards, and promoting its methodologies across

member states. Replicating CHESS cross-regional collaboration model would further unify European cybersecurity ecosystem.

CHESS has proven that regional collaboration drives significant advancements in cybersecurity. Its true success lies in sustaining and scaling these outputs. By institutionalizing its frameworks, fostering stronger partnerships, and embedding its solutions into European strategies, CHESS can serve as a blueprint for the future of cybersecurity collaboration. The work done so far is a testament to the power of shared goals and collective action. Now, it is up to stakeholders at all levels to carry these achievements forward, ensuring that CHESS legacy continues to shape a safer, more resilient digital Europe.