CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

D2.1
Mid-term Report on Training and Mobility

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	D2.1
Deliverable name	Mid-term Report on Training and Mobility
Lead Beneficiary	BUT
Type	R — Document, report
Dissemination Level	PU - Public
Work Package No	WP2
Date	19 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.

Editor

- Jan Hajný (BUT)
- Lisa Morávek (BUT)

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)
- Martin Ukrop (Red Hat)
- Pavel Čeleda (MUNI)
- Mariia Bakhtina (UTARTU)
- Petr Muzikant (CYBER)
- Antonín Dufka (MUNI)
- Jan Kvapil (MUNI)
- Lukáš Daubner (MUNI)
- David Halasz (MUNI)
- Hendrik Pillmann (RIA)

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

AI/ML – Artificial intelligence/machine learning
BDHKE – Blind Diffie-Hellmann Key Exchange
BUTCA – Brno University of Technology Cyber Arena
CA – Challenge Area
CERT-EE – Estonian Computer Emergency Response Team
CHESS – Cyber-security Excellence Hub in Estonia and South Moravia
CRoCS – Centre for Research on Cryptography and Security
CSIRT – Computer Security Incident Response Team
DLP – Data Loss Prevention
ECDSA – Elliptic Curve Digital Signature Algorithm
ECSC – European Cybersecurity Challenge
F4SLE – Framework for Security Level Evaluation
FEKT – Faculty of electro technology at BUT
FIPS – Federal information processing standards by NIST
ICT – Information and Communication Technology
IEEE – Institute of Electrical and Electronics Engineers
IOHK – Input Output: Blockchain infrastructure research engineering company
IoST – Internet of Secure Things
ITS – Intelligent Transportation Systems
KPI – Key Performance Indicator
KYPO – Cybernetic polygon Cyber range platform of MUNI
MASS – Measurement Application for Self-assessing Security
NCSC-EE – National Cyber Security Center
NGO – Non-Governmental Organisation
NUKIB – Czech National Cyber and Information Security Agency
OA – Open Access
R&I – Research and Innovation
TA – Target Audience
WP – Work Package

Executive Summary

One of the strengths of the CHESS consortium is its cross-sector and cross-regional nature, which allows for knowledge transfer and forms the basis of CHESS training and networking objectives. In the first 24 months of the project, several workshops, seminars, train-the-trainer events and conference contributions have been organised by CHESS to upskill and train hundreds of participants from all sectors of the quadruple helix on cybersecurity-related topics across the six challenge areas in CHESS. These include consortium internal events, cross-regional and cross-sector training, technology transfer days as well as international summer schools and workshops at conferences.

We organised multiple events in various formats with participants from the private and public sectors, national security agencies, and academia. Through training for educators and teachers, CHESS hopes to generate a wider outreach on a basic level, whereas conferences like the "Future Cryptography Conference" bring together experts from industry and academia to discuss highly specific topics. Especially the events that bring together commercial and academic realms have proven very successful, with many attendees participating in regional and cross-regional events between South Moravia and Estonia. In total, the number of attendees and events is higher than was projected in the project proposal's KPIs and is a testament to the broader interest in cybersecurity related topics and training opportunities.

The present report 1) outlines the training focus across all six challenge areas of CHESS, 2) presents the various events hosted by CHESS, and 3) draws conclusions on their success and the implications for future activities in WP2 focused on skills development actions.

Table of Contents

1. Introduction

Cybersecurity is a rapidly evolving field that greatly depends on the upskilling and education of professionals to protect companies and the public from current and future electronic attacks. The CHESS consortium, as a cross-regional and cross-sector alliance, places great focus on the training and knowledge exchange not only of its partners but beyond the consortium as well.

One of the key **objectives** of the CHESS project is to raise awareness and spread knowledge on cybersecurity in both South Moravia and Estonia, as well as to train members of the public, academia, and related industries. The consortium organises various training events and workshops **to build skills for ecosystem actors** across all four sectors of the quadruple helix. These events, as well as networking opportunities, **promote mobility and technology transfer within the ecosystem** and **increase the international reputation of CHESS** by providing excellent training open to global audiences (Objectives O2.1, O2.2 and O2.3).

In order to meet the above-mentioned objectives, different forms of awareness-raising and training events are organised by the partners of the CHESS consortium, including **Training the Trainer** events to increase the outreach by providing training to educators of cybersecurity, thus reaching more individuals eventually (T2.1). Another focus lies on **cross-regional** knowledge sharing through seminars and workshops that are being held across all six Challenge Areas in Estonia and the Czech Republic (T2.2). Also, a special focus is placed on technology transfer, which is promoted additionally through specific Industrial Days and **Technology Transfer Days** (T2.3). In addition, CHESS hosts international training schools and workshops to build its reputation (T2.4), especially in the academic world.

As a second pillar of the CHESS training and knowledge-sharing effort, a mobility scheme was put in place to facilitate **staff exchange and fellowships** between all CHESS partners during the entire course of the project (T2.5). This offers seasoned researchers a new perspective and new opportunities for collaboration while helping first-stage researchers to gain experience in a new setting.

This report outlines the measures taken in all of these training formats so far, drawing conclusions on their success and giving an outlook on future activities within *WP2 Skills Development Actions for Cybersecurity R&I Ecosystem*.

2. Challenge Areas: Priorities and Training Focus

2.1. Challenge Area 1: Internet of Secure Things (IoST)

CA1 acknowledges the continuous expansion of the IoT which makes securing the myriad of connected devices increasingly critical. This CA focuses on developing robust security protocols, standards, and solutions to protect IoT devices and networks from cyber threats. When developing IoST systems, we consider the use of state-of-the-art measures and best practices (e.g., ones reported in academic publications).

With regard to training, we aim to share interdisciplinary research connecting privacy to law, formal modelling, policy, and data privacy management. We promote collaboration with research institutions to help navigate state-of-the-art security and privacy countermeasures. Training events that focus on IoST aim to transfer best practices and state-of-the-art cybersecurity approaches and cryptography tools into practice. Reaching a broad audience across all four sectors, the necessity to create a matrix of security and privacy properties and priorities defined by stakeholders in IoST and ITS fields is promoted. This includes designing an IoST considering the need for interoperability with external systems and partners.

A key event promoting our advances in CA1 is the International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), previously funded by the SPARTA project and continued under CHESS (more information below).

2.2. Challenge Area 2: Security Certification

CA2 addresses the need for standardised security certifications that can provide assurances of security levels for products, systems, and services. Security certification plays a crucial role in building trust among users and is vital for the adoption of new technologies.

The main training interests in CA2 include hands-on training on security certification frameworks, such as the SCRUTINY framework. Developed by MUNI, it automates the verification of security products such as smartcards delivered to the end-user, analysing the Common Criteria and FIPS certification documents using *sec-certs*. Moreover, we are interested in creating a clear certification roadmap for cryptographic modules and creating a clear roadmap on how to achieve the requirements set by the recent EU legislation.

2.3. Challenge Area 3: Verification of Trustworthy Software

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

Our focus for training lies in cross-border knowledge exchange between academic and industrial sectors, using the existing tools for formal verification and analysis of software systems and identifying real-world problems of software development companies via tech transfer days and short-term staff exchange. The CA3 team is also interested in evaluating software tools for technology transfer developed by the key stakeholders and identifying the missing functionality and crucial limitations of state-of-the-art formal methods.

2.4. Challenge Area 4: Security Preservation in Blockchain

CA4 is dedicated to advancing the blockchain domain through research, development, and knowledge dissemination. CA4 aims to examine blockchain security, identify security risks, and enhance blockchain applications' resilience against various vulnerabilities. CA4 also focuses on creating tools and frameworks for security risk management in decentralised systems, emphasising privacy-enhancing cryptographic techniques like zero-knowledge proofs, threshold cryptography, and privacy-preserving transaction protocols.

Moreover, CA4 prioritises training programs to build expertise in blockchain security among professionals and researchers, addressing an industry-wide need for skilled practitioners. By raising awareness of blockchain, CA4 ensures blockchain's long-term role in secure digital transformation and promotes it as a trusted technology in various sectors. Following are the key activities, outcomes, and potential impacts we focus on in training efforts under CA4.

- **Addressing Security Challenges:** Specific attention is given to addressing blockchain security challenges and vulnerabilities, such as Sybil attacks and smart contract vulnerabilities. These efforts focus on strengthening application-level security through new detection and prevention strategies tailored to the blockchain and decentralised applications.
- **Threshold Cryptography on Secure Hardware:** Utilising threshold cryptography, computed on secure hardware, enables multi-party computations without revealing participant data. This exploration aims to improve blockchain applications where sensitive data protection is important.
- **Statistical Analysis of Coinjoin Protocols:** Analysing privacy-focused protocols like Coinjoin allows for deeper insights into the statistical vulnerabilities of mixing mechanisms. This ensures the protocol's robustness while reinforcing its application in privacy-preserving blockchain networks.

The training activities under CA4 are designed to contribute significantly to blockchain's security, resilience, and trustworthiness. By helping to develop blockchain-specific security frameworks, risk mitigation tools, and privacy-enhancing protocols, CA4 contributes to a secure, more compliant, and sustainable blockchain ecosystem, fostering trust in decentralised applications.

2.5. Challenge Area 5: Post-Quantum Cryptography

CA 5 is focused on research, development, training and awareness raising in the area of post-quantum cryptography. The main objective is to design, implement and verify

technologies that are resistant to attacks by quantum computers. In particular, CA5 is focused on digital signatures, authentication and identification protocols and systems for network data encryption. Since the start of the CHESS project, most CA5 activities were focused on cryptologic protocol design and experimental verification, where the presence of two distant countries in the consortium can be effectively used, for example for pilot evaluation of long-distance secure connections.

As post-quantum cryptography is a rather new discipline, where new algorithms and protocols only emerge, it is of crucial importance to support training and awareness activities in this field. The Estonian and Czech partners in the consortium have rather different expertise in this field, for example Cybernetica from Estonia is more focused on algorithms and protocols for eGovernment solutions, while Brno University of Technology has rich experience in communication technologies and networking. Therefore, within the CHESS project, it makes sense to combine this expertise and support networking, internships, joint workshops and other events that lead to knowledge sharing.

Furthermore, CA5 participated on numerous summer schools and workshops, where latest developments and technologies were introduced to raise awareness and ignite discussions. The presentations from CHESS CA5 members are subject to the CHESS dissemination report. In the following sections, the description of concrete events organised within CA5 is provided. Some of the events were co-organised with other CAs for efficiency and complementarity reasons.

2.6. Challenge Area 6: Human-Centric Aspects of Cybersecurity

In CA6, the training component includes hands-on workshops utilising the open-source interactive learning platform KYPO[1]. It is used to equip both cybersecurity students and early-career professionals with essential skills through scenario-based hands-on learning.

The collaboration between South Moravia and Estonia creates opportunities for mutual growth. South Moravia can tap into Estonia's established cybersecurity training and certification expertise, while Estonia benefits from South Moravia's innovative approaches and technologies to cybersecurity education. Workshops require instructors skilled in both technical and interpersonal areas to support well-rounded learning.

Tabletop exercises provide realistic, interactive cybersecurity scenarios that foster collaboration and decision-making under pressure. These exercises are valuable for both technical and strategic skill development, enabling organisations to improve incident response capabilities and refine security policies.

Additional workshops focus on the penetration testing process, offering insights for technical professionals and those managing cybersecurity strategies, encouraging cross-sector knowledge exchange among cybersecurity experts.

[1] https://crp.kypo.muni.cz/

3. Events Organised

During the first 24 months of the project, various training events were organised for the CHESS project. These span all six challenge areas and have reached audiences from all four sectors. Some of the events presented below were planned and hosted fully by CHESS, while others have been organised by third parties but included a CHESS training event. All of these training and education events have been included in this report, but not all count towards our KPIs related to knowledge-sharing (see table below).

KPI No.		M24	M48
5	# of Training/education events organised (summer schools, workshops)	6	14
6	# of Trained researchers	30	120
7	# of Trained users from industry	20	80
8	# of Trained users from NGOs	15	40

The events we include in CHESS KPIs 5-8 are only international or cross-regional events organised or co-organised by CHESS targeted at researchers, industries and NGOs and open to wider audiences beyond the CHESS consortium. The events in the report that fall under this definition are marked visibly in the tables that list organised events in each section.

The following report divides all the events according to the tasks defined for *WP2 Skills Development Actions for Cybersecurity R&I Ecosystem* in the GA, thus splitting them up into "Training on cybersecurity training" (T2.1), "Cross-regional knowledge transfer events" (T2.2), "Technology transfer days" (T2.3), "International workshops and conferences" (T2.4). Our activities have caught the attention of different stakeholders from our regions. Therefore, we have organised several regional events across different sectors. While these do not count towards our KPIs directly, as they are not cross-regional or international, they still have a great value in sharing knowledge between sectors and promoting CHESS.

3.1. Training on Cybersecurity Training

In order to reach a greater number of professionals and the public, CHESS training events include train-the-trainer events that cascade knowledge and promise a wider outreach. They target students, educators and teachers in secondary schools and universities.

In the first two years of the CHESS project, multiple training events on cybersecurity were carried out within the challenge areas CA5 and CA6.

BUTCA Teacher Training
22 October 2024, Brno, Czech Republic

The training of trainers and teachers in cybersecurity is an important yet often neglected activity. It needs to begin very soon, so that we have enough experts that are able to train and teach the next generation. Of course, it is not possible to always start with complex topics, such as post-quantum cryptography (CA5), on all levels (in particularly high schools).

Therefore, we have started with introductory training activities in cybersecurity for high school teachers. For this purpose, BUT organised a "train the trainers" workshop on efficient cybersecurity trainings for high-school teachers on 22 October, 2024. The workshop was focused on new methods of teaching, including novel approaches using gamification and interactive activities. Concrete tools, materials and techniques were shown during the event. New trends in cryptography and cybersecurity, including PQC, were introduced as well. This "train the trainers" event was attended by 15 high school teachers and served as a preliminary activity for more-specialised events of this type, including the deployment of post-quantum technologies, planned for 2025. The event is depicted below.

With CA 6 focusing on the human aspect in cybersecurity, many training events in this CA aim to inform and educate educators who then spread the word. In 2023 and 2024 these events included the following.

Online cybersecurity training for students (2023 and 2024)
Aug 2023 and Sept 2024, online

Members of the Czech national team and other national teams (35 students from 6 countries) qualified for the ECSC 2023 and played hands-on games to train their cybersecurity skills, comparing their scores to foster a competitive edge. This training helped them to develop strategic thinking and technical expertise, which they later leveraged in their participation in the ECSC 2023. Notably, these teams had qualified for the ECSC through rigorous selection processes, demonstrating their advanced abilities and commitment to excellence. A similar **online training for members of national teams of the Czech Republic** and other national teams was held **in 2024**. 70 competitors from 11 European countries again played hands-on games to train their cybersecurity skills and prepare them for their participation in the European Cybersecurity Challenge 2024.

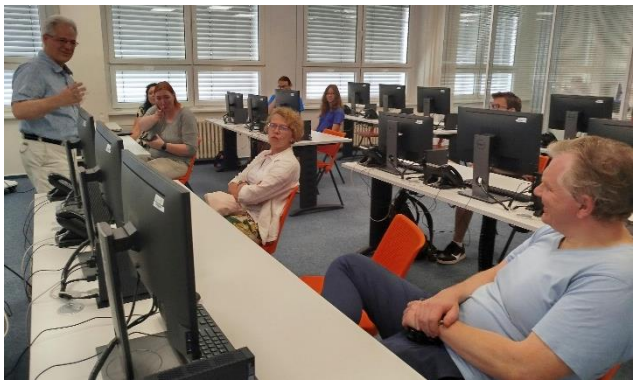
Exercise Platform – Train the Trainers
5 June 2024, Brno

The CA6 team at MUNI held the first training event for trainers, introducing the INJECT exercise platform[2] to local stakeholders from industry and project partners in the Czech Republic.

Hands-on workshop on cybersecurity training
26-27 June 2024, Brno

In June 2024, cybersecurity educators from Estonia visited Masaryk University and participated in the hands-on workshop designed to provide participants with an overview of tabletop exercise types, their necessity, benefits and best practices. Participants were introduced to the INJECT Exercise Platform for conducting cybersecurity tabletop exercises. An existing tabletop exercise was tested during the workshop. The participants discussed designing, conducting, and evaluating tabletop exercises. Also, they planned how to leverage and contribute to tabletops in CHESS, including the possibility to design open-source tabletop scenario(s) in Estonia using the INJECT platform.

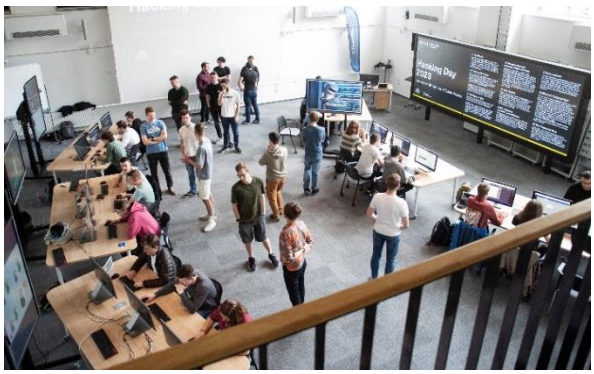
During their visit in the Czech Republic, the Estonian educators, accompanied by colleagues from MUNI, visited Čichnova technical high-school school in Brno. The aim of the visit was to speak to Czech high-school teachers and students, exchange experience and knowledge on teaching cybersecurity, while advertising for future job opportunities in this realm. Also, participants discussed future collaboration between Brno high-school and two Estonian high-schools: Tallinn Polytechnic School and Kehtna Kutsehariduskeskus in Raplamaa.



[2] https://inject.muni.cz/

MUNI Hacking Days (2023, 2024)
11 May 2023, 12 December 2023, 14 May 2024, Brno and online

The events featured cybersecurity games created by students from the Cyber Attack Simulation Seminar at MUNI, giving novices and experts a chance to practice their ethical hacking skills. Participants played attack-only cybersecurity games featuring recent and popular attacks and vulnerabilities. The events were organised onsite at Masaryk University for Czech participants and in parallel online for students and educators in Estonia. 126 students participated in these events.



Cybersecurity Summer School (2023, 2024)
August 2023 and June 2024, Brno

The goal of the events was to select and train a Czech team to represent the Czech Republic in the European Cybersecurity Challenge (ECSC) competitions. During the summer school days, young participants solved various tasks to demonstrate their skills. The CHESS team organised cybersecurity games and practical workshops for talented students, helping them develop the skills needed for the European finals.

Tabletop training at TalTech and Tallinn Polytechnic School
November 2024, Tallinn, Estonia

A senior researcher from Masaryk University visited Tallinn and with the support of TalTech university staff held cybersecurity training for university students at TalTech and one training workshop for vocational school students and teachers from Tallinn Polytechic School and Kehtna Kutsehariduskeskus. The cyber exercises were hosted on the Masaryk University Cybersecurity Laboratory's INJECT Exercise Platform. Also, during his visit to Tallinn, the MUNI researcher had a presentations at TalTech followed by discussions about teaching cybersecurity, with a particular focus on incorporating tabletop exercises into cybersecurity courses.

Table 1: Training in Cybersecurity Training events hosted by CHESS

	Name of event	Partners	CA	Acad.	Industry	NGO	Stu.	Other
1	BUTCA Teacher Training December 2024	BUT	CA6 CA5	5				15
2	Online cybersecurity training for students 2023	MUNI	CA6				35	
3	Online cybersecurity training for students 2024	MUNI	CA6		3	2	60	7
4	Exercise platform – Train the trainers (2024)	MUNI	CA6	12	4			6
5	CHESS hands-on workshop on cybersecurity training	MUNI, TalTech	CA6	4				4
6	2 MUNI Hacking Day 2023	MUNI	CA6				83	
7	MUNI Hacking Day 2024	MUNI	CA6				43	
8	Cybersecurity Summer School 2023	MUNI	CA6				25	
9	Cybersecurity Summer School 2024	MUNI	CA6				30	
10	Tabletop training TalTech, Tallinn, 2024	MUNI, TalTech	CA6	2			14	
11	Tabletop training vocational schools, Tallinn, 2024	MUNI, TalTech	CA6				41	7

3.2. Cross-Regional Knowledge Sharing

A crucial benefit of CHESS is the possibility to transfer knowledge between Estonia and South Moravia. We leverage this benefit by organising joint events where experts from both Estonia and South Moravia participate and share their experience and knowledge with other experts from academia, the public sector and industry.

Future Cryptography Conference"[3]
13 May 2024, Tallinn, Estonia

A very successful event with more than 80 participants was co-organised by the Estonian Academy of Sciences, the Estonian Information System Authority (RIA) and Cybernetica. Speakers from CHESS from both Estonia and Czechia were part of the program, speaking about the post-quantum transition and raising awareness across sectors. The participants discussed how to use mathematics to protect the secrets of governments, companies and individuals against future technologies.

The inaugural Future Cryptography conference focused on post-quantum cryptography (PQC), a group of technologies that the quantum computers foreseen today will not be able to breach. We heard several talks about standards, applications and migration strategies by scientists and government stakeholders from Estonia and Czechia.

Post-Quantum Cryptography Workshop

4 December 2024, Prague, Czech Republic

Following the successful format of the Estonian Future Cryptography Conference mentioned above, Czech partners organised a smililar event when speakers from both Czechia and Estonia were present. This time, the focus of the event was specifically targeted at PQC transition in the governmental sector. The event was attended by ca. 50 experts from government agencies in Estonia, Slovakia and the Czech Republic as well as industry representatives from both regions. This workshop organised by BUT showcased how the CHESS project increases cross-sectoral and cross-regional collaboration in post-quantum transition efforts.

CA2 Workshops dedicated to sec-certs tool
May and June 2023 in Tallinn, Feb 2023 online

IN CA2 collaboration across regions has been very close, with the MUNI team holding several workshops showcasing their sec-certs tool[4] in Estonia. First, researchers from MUNI, from the Centre for Research on Cryptography and Security (CZ) visited Tallinn in May 2023 to present at the workshop titled "Practical use of security (CC, FIPS 140) certificate data mining for vulnerability monitoring and assessment: **Toolbox presentation (Sec-certs)".** This event was visited by 27 Participants, including professionals from RIA, the University of Tartu and GuardTime.

[3] The complete program and photos from the event is available on conference webpage: https://futurecryptography.eu/.
[4] https://seccerts.org/

An **Online workshop for Cybernetica,** towards more transparent security certifications included the presentation of the sec-certs tool by Petr Švenda from MUNI on 2 February 2023.

Moreover, a **workshop in Tallinn for Estonian Computer Emergency Response Teams** on 15 June 2023 as a part of CERT-EE (Symposium) 2023 was visited by 292 participants (41% public sector, 34% private sector; 12% academy; 13% Other) that attracted a high amount of international audience (47% international background).

Cyber security experts and professionals from related disciplines in government, academia, police and the private sector were encouraged to attend in order to ensure a broad-based, interdisciplinary atmosphere to examine the growing connection between computer security, national security and cybercrime. The 2023 0ct0b3rf3st (Symposium) on incident response continues the traditions of community events that CERT-EE has held in previous years.

Workshop on practical cybersecurity certification
19 March 2024, Tallinn

An especially fruitful workshop about practical cybersecurity certification took place on 19 March in Tallinn. Two experts first gave a talk and then participated in further discussions with the participants. The presenters were:

- Miguel Bañón (Spain): Expert in cybersecurity evaluation and certification, regulation, policy and standards development. Designer and developer of cybersecurity evaluation and certification schemes and labs in Europe. Miguel talked about the ISO/IEC 15408 series, potential development of new protection profiles (PP) and how the recently adopted EUCC changes the rules of the game.
- Clemens Wanko (Austria): Head Trust Infrastructure Division in TÜV TRUST IT. Clemens talked about product versus process certifications, how to integrate CC/FIPS140 certified products in eIDAS compliant eID or Trust Services.

The event started with Miguel Bañón's keynote "Using the ISO/IEC 15408 for certification and how the EUCC rules are changing the certification game" was followed by an hour-long discussion on strategies for certifying new cryptographic products with CC/EUCC, including writing new protection profiles. We talked about what the most effective way is for the market to agree on new protection profiles for security products and which tools one can use to reduce the cost of certification and improve its security guarantees. After lunch Clemens Wanko gave his keynote on "Product versus process certifications, how to integrate CC/FIPS140 certified products in eIDAS compliant eID or Trust Services". This was followed by a discussion on how EU member states and companies can tackle the incoming wallet providers' need to certify and whether we will need separate certification targets for purely software and hardware-software hybrid technologies like digital signatures, post-quantum and secure computing.

The participants from public sector organisations wanted to understand how to set up evaluation and certification in Estonia for the long run, what the resource requirement is for product certification through CC, as well as other European systems, and to clarify the Estonian need for certified cryptography.

The participants had a deep knowledge of security and cryptography (security engineers, scientists, architects), some with a business background and knowledge of eID and certification. Some participants had knowledge about eIDAS2 and security evaluation and Common Criteria, but few people had had hands-on experience with writing ST documents and working with CC evaluators. In the near future, the participants are expected to have to participate in upcoming product certification projects.

RIA CyberMeetUp workshop
16 May 2024 Tallinn and online

The RIA CyberMeetUp took place on 16 May, 2024, at the Palo Alto Club in Tallinn, hosted by the Republic of Estonia's Information System Authority (Riigi Infosüsteemi Amet - RIA). From CA4, Antonín Dufka and Jan Kvapil, PhD candidates from Masaryk University in the Czech Republic, presented on the "MeeSign: Threshold Cryptography Platform and Its Applications Beyond X-Road." Their talk covered the fundamentals and applications of threshold cryptography, including an overview of MeeSign—a demonstration platform. Participants engaged in a practical session, working hands-on with MeeSign to explore its use in secure, distributed systems. The event drew a live audience of over 30 professionals from the cybersecurity industry. Additionally, the event was streamed online, attracting considerable attention and having 350 views.

Threshold cryptography workshop at UT
23 May 2024, Tartu, Estonia

Two Czech junior researchers from Masaryk University, using the CHESS fellowship scheme, held a Threshold Cryptography Workshop at the University of Tartu, Institute of Computer Science for students, faculty and representatives of industry with over 30 attendees. The workshop offered practical illustrations of how threshold cryptography enhances security in current cryptographic systems. Using a hands-on demonstration platform, they explored real-world scenarios where threshold cryptography could be applied, sparking engaging discussions and interactive activities[5].

[5] The workshop slides can be accessed here: https://chess-eu.cs.ut.ee/2024/05/24/meesign-threshold-cryptography-platform/

During the workshop, the two students also connected with local PhD students, discussing their studies and research topics in an informal setting, further strengthening academic exchange and collaboration.

Mastering Penetration Testing Reports Workshop
2-3 November 2023, Tallinn and Tartu

Cybernetica, in collaboration with MUNI organised one workshop in Tallinn on 2 November 2023, and another one in Tartu on 3 November 2023. The target group consisted of cybersecurity specialists, defined as individuals working in technical cybersecurity roles at companies that provide penetration testing as a service.
We worked with a demonstration of a standard penetration testing report – the demonstration focused on what lies behind the penetration testing report, providing all participants with the same baseline for further discussion and evaluation. The goal was to show participants how a specific penetration test scenario is conducted, enabling them to assess the content of the vulnerability finding in the report and identify what they would prefer to see included.
Five vulnerabilities were presented, along with demonstrations of their exploitation.
The events were tailored to cater to a diverse audience, ranging from technical professionals such as developers, validators, and administrators, to cybersecurity managers and decision-makers. The workshops aimed to provide valuable insight into the process of penetration testing for both people involved in the technical aspects and for individuals overseeing cybersecurity strategies. It further offered an overview of what is happening before receiving the penetration testing report. It dealt with organising focus groups to get feedback from cybersecurity experts about the pain points of penetration testing and thus contribute to the research that focuses on improving the usability of penetration testing reports.
This workshop created an opportunity for cybersecurity professionals from different sectors to meet and share their experience with penetration testing.

InfoSec seminar
25 October 2024, Tartu

During his fellowship, one researcher from the Czech Republic held a workshop at UTARTU. In their InfoSec seminar 8 InfoSec group researchers discussed "Forensic Readiness & Privacy: Conflicts and Resolutions" and privacy-preserving vehicle sharing and intermediate results.

Knowledge-sharing seminars at MUNI FI and BUT FEKT
October 2024, Brno

With the rise of hyperconnectivity, we see a number of smart solutions enabled for users, starting from smart transportation solutions, e-health, e-governance, and up to Industry 4.0. While such solutions heavily rely on collaborative data exchange between partnering organisations, integrating used-to-be standalone systems poses information security risks and may threaten privacy. Mariia Bakhtina, during her doctoral studies, developed a method for managing information security and privacy management for organisations participating in smart solutions delivery. The method mainly focuses on assuring data protection and security of exchanged data based on the defined trust assumptions. So, the seminars Mariia conducted at MUNI FI and BUT FEKT focus on the "Method for Information Security and Privacy Management in Smart Solutions."

Seminar #1 was organised at MUNI FI

The CRoCS (Centre for Research on Cryptography and Security) seminar, held on 1 October, 2024, gathered an audience of 15 attendees, including MSc and PhD students and CRoCS staff members. This focused seminar provided an engaging platform for academic exchange, with in-depth discussions on information security and privacy management in smart solutions. Attendees actively participated, sharing insights and exploring new perspectives in cybersecurity research, making it a valuable experience for students and researchers.

Seminar #2 was organised at MUNI FI

The LaSArIS (Lab of Software Architectures and Information Systems) seminar on 3 October, 2024, welcomed 14 participants, including MSc and PhD students and LaSArIS staff members. The session provided an engaging platform for students and faculty to exchange ideas, discuss research, and explore projects within smart solutions' information security and privacy management.

Seminar #3 was organised at BUT FEKT

On 10 October, 2024, a seminar was held with a focused audience of seven attendees, specifically the BUT FEKT staff members. The event provided an intimate setting conducive to in-depth discussions, allowing participants to engage deeply with the material and share insights related to the seminar's topic. The small group fostered a collaborative atmosphere, encouraging open dialogue and sharing expertise among academic staff related to information security and privacy management in smart solutions.

Table 2: Cross-regional events to exchange knowledge between South Moravia and Estonia

	Name of event	Partners	CA	Acad.	Industry	NGO	Stu.	Other
1	Future Cryptography Conference 2024*	RIA, BUT, CYBER	CA5	10	58		2	13
2	Post-Quantum Cryptography Workshop 2024*	BUT, CYB, MUNI, RIA	CA5 CA1	20	15			17
3	Toolbox presentation (sec-certs) at RIA 2023	RIA, MUNI	CA2	27 participants including people from RIA, UTARTU, GuardTime				
4	Online workshop for Cybernetica (sec-certs) 2023	CYBER, MUNI	CA2		15			
5	Workshop for Estonian Computer Emergency Response Teams 2023	MUNI, RIA	CA2	35	99	120 public	38	
6	Workshop on practical cybersecurity certification 2024*	CYBER, MUNI, RIA	CA2	0	20	5	0	
7	RIA Cyber meet-up in Tallinn 2024	RIA, MUNI	CA4		30			350 online
8	Threshold Workshop 2024	UTARTU, MUNI	CA1, CA4		5		25	
9	Mastering Penetration Testing Reports Workshop Tartu 2023*	CYBER, MUNI	CA6	3	8			4

10	Mastering Penetration Testing Reports Workshop Tallinn* 2023	CYBER, MUNI	CA6	2	8		1	7
11	InfoSec Seminar 2024	UTARTU, MUNI	CA2	8				
12	3 Privacy Management Seminars 2024	MUNI, BUT, UTARTU,	CA1, CA4	21			15	

3.3. Regional Events Across Various Sectors

Using the knowledge gained in cross-regional events and through international collaboration, some events are held regionally to spread knowledge among stakeholders and representatives of different sectors. These include representatives of critical infrastructure (water works, hospitals etc), educators, and tech companies. These events address members of all four sectors and they are comparable to T2.3 Industrial Days with the exception of not being cross-regional and not being necessarily hosted at the premises of a CHESS member organisation. The following section presents the events held locally in South Moravia or Estonia and spanning various sectors.

PROTECT 24: The Current and Future Roles of AI in Protecting Critical Infrastructure
15 November 2024, Brno

The workshop focused on the current and future roles of AI in improving the methods for protecting critical infrastructure and other designated areas. The workshop brought together researchers and practitioners in the field and provides an informal platform for exchanging ideas and initiating new collaborations.

The workshop addressed the following key issues:

- The current methodology for protecting critical infrastructure and other designated areas. What are the best practices and the main problems?
- What is the envisioned role of artificial intelligence and robotic devices? How should AI interact with humans? Is our legislation ready?
- What state-of-the-art AI methods are ready to deploy? What are their benefits? What can be expected in the near future?

The core of the topic was physical security, for example, security of the building, where experts from the Faculty of Informatics are able to calculate optimal randomisation strategies, when and where the security patrol should go. The purpose was to bring together experts from academia, customers (such as the state organisation responsible for operation of national railways or the operator of the electricity distribution network) and security providers, i.e. security agencies.

CA2 F4SLE training events
Multiple events in 2024, Tallinn and Tartu

In CA2, specific F4SLE-related trainings were held, mostly not as stand-alone events but integrated into a suitable training day or seminar of a specific community. Such an approach has made it possible to reach a larger audience and show the use and need of F4SLE precisely when the more general topic of information security management implementation is in the background. However, such events are very community-centric and therefore materials are not shared publicly. F4SLE-related training events in CHESS include the following:

F4SLE results interpretation seminar included into sectoral info days (Q4 2023, held 3 times).
In total, there were information days for three sectors (water and district heating companies (partially online), hospitals and transport companies), before which at least 5 of the participating organisations had to fill out the F4SLE questionnaire. The results were interpreted based on the sector and information security recommendations were distributed on this basis.

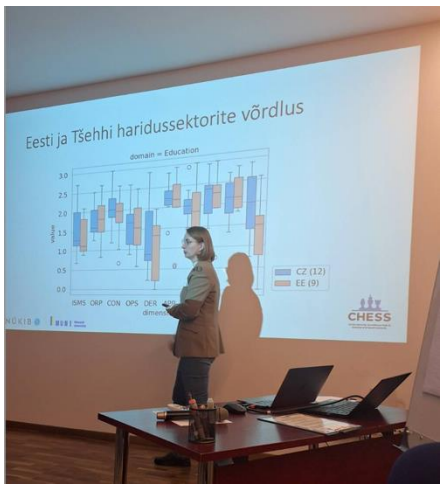
A **F4SLE intro was included to cybersecurity management trainings for the Climate ministry and Culture ministry subordinate institutions in August 2024**

Internal closed trainings of the institutions with guest speakers, where the emphasis was primarily on the implementation of information security management, but recommendations were shared to evaluate regularly security level and F4SLE was introduced for that.

Cybersecurity management training for education technologists included F4SLE usage (August 2024)

A multi-day Estonian meeting on education technologists, where many topics were discussed. The workshop of information security management topics made it possible to give short instructions and test for the use of F4SLE in schools[6].

Information security standard implementation training day included F4SLE slot (October-November 2024; 2 similar seminars)
Introduction of F4SLE, as well as its usage instructions and interpretation of the results so far, during the information security management implementation involvement seminars.



“Lunch and learn" workshop
25 June 2024, Brno

The workshop was held at Red Hat where Perun, a performance versioning and dynamic analyser being developed by BUT and MU was presented. The project team developed a new (now public) Perun hands-on demo for the event to showcase Perun's capabilities and potential applications. The event ran in two phases, first with an audience of interested Red Hat developers (around 15 participants) and then a dedicated run for a kernel quality engineering team that was identified as currently having the highest potential of integrating Perun in their work (around 10 participants).

Blockchain workshop at Küberinnovatsioon (Cyber Innovation) conference
14 June 2023, Tartu

The "Küberinnovatsioon 2023 Tartu" conference[7] took place on 14 June at the University of Tartu's Institute of Computer Science, Delta Center, bringing together IT, information security, and cybernetics enthusiasts. A total of 113 participants registered from diverse backgrounds, including students, researchers, industry professionals, representatives from

[6] Internal agenda and presentations: https://haridustehnoloogid.ee/kehtnas-toimus-uleriigiline-eesti-haridustehnoloogide-liidu-suvekool/)
[7] Conference website and program: https://kuberinnovatsioon.cs.ut.ee/2023-2/

government institutions, and university administrative staff. The conference includes presentations, hands-on workshops, and student project presentations. The day concluded with a special evening gathering organised by Guardtime in Gutenberg Hall in Aparaaditehas. This event created a collaborative atmosphere for discussing cutting-edge trends in cybersecurity and innovation, strengthening connections within the tech community.

At this conference, the CA4 team from UT organised a blockchain workshop. The workshop's agenda included a comprehensive introduction to blockchain and its essential elements. The workshop also covered the fundamentals of blockchain and cryptocurrency, explaining core characteristics like decentralisation, immutability, and transparency. It offered a hands-on guide to writing, compiling, and deploying smart contracts, making it practical for those aiming to build on blockchain[8].

Table 3: Training events held across various sectors

	Name of event	Partners	CA	Acad.	Industry	NGO	Stu.	Other
1	PROTECT24	MUNI	CA3	19	9			23
2	F4SLE results interpretation seminar included into sectoral infodays 2024	UTARTU, RIA	CA2		80+20 +10			
3	F4SLE intro included to cybersecurity management training to Climate ministry and Culture ministry subordinate institutions 2024	UTARTU, RIA	CA2		50+20			
4	Cybersecurity management training for education technologists included F4SLE usage 2024	UTARTU, RIA	CA2		22			
5	Information security standard implementation training day included F4SLE slot 2024	UTARTU, RIA	CA2		3x40			
6	Blockchain workshop at Küberinnovatsioon 2023		CA4	113 researchers, students, industry professionals, governmental organisation				

[8] Workshop slides: https://chess-eu.cs.ut.ee/2023/06/22/blockchain-workshop/

7	Lunch-n-Learn 2024	Redhat, MUNI, BUT	CA3	3	25			

3.4. Technology Transfer Days

To improve collaboration between companies and academia, task T2.3, **Hosting Technology Transfer Days,** aims at hosting Technology Transfer Days. These events are designed specifically to exchange knowledge primarily between academic and industrial organisations hosted on the site of different CHESS partners, who will demonstrate specific technologies or techniques.

CHESS Industrial Day 2023
8 December 2023, Brno

Masaryk University and Brno University of Technology organised a pilot event called CHESS Industrial Day 2023 at the Faculty of Informatics, at Masaryk University.
The aim of CHESS Industrial Day 2023 was to bring together researchers and practitioners in formal methods from industry and academia. The event provides an informal platform for exchanging practical experience with methods and tools for software analysis/verification/testing, and discussing their benefits and bottlenecks. There were around 43 participants mainly from the industry (RedHat, Honeywell, Certora, Oracle) as well as MUNI, BUT, and Tartu University.

The CHESS Industrial Day 2024
9 December 2024, Tallinn

This one-day seminar brings together researchers in academia with colleagues from industry, with a focus on companies operating in Estonia and Czechia. The focus is the use of software verification and formal methods in the industry, the current challenges, the shortcomings of current approaches, and the opportunities for collaboration and knowledge and technology transfer. The meeting features presentations from CHESS industrial

partners, including Guardtime and Cybernetica, as well as discussions and opportunities for networking.

Table 4: Technology Transfer days

	Name of event	Partners	CA	Academia	Industry	NGO	Other
1	CHESS Industrial Day 2023	MUNI, BUT	CA3	28	15		
2	CHESS Industrial Day 2024	Cybernetica, GuardTime	CA3	12	3		

3.5. International Training Schools and Workshops

Some of the CHESS training and education events have an even further outreach due to them being open beyond the two regions of South Moravia and Estonia. Usually, these are conferences or training events for students and researchers, but they can include members of the public and private sector, too. The following gives an overview of such events, e.g. workshops held at international conferences.

CHESS workshops at Estonian Summer School in Computer and Systems Science
14-16 August 2023, Tartu

The 20th ESSCaSS: The Estonian Summer School in Computer and Systems Science (ESSCaSS 2023) was held on the 14-16 August at the Institute of Computer Science at the University of Tartu Delta Centre. It brought together more than 120 researchers and doctoral and master students from Estonia, the Czech Republic and other countries.
Below are the highlights of the CHESS Cyber-Security Excellence Hub-related training and research activities at ESSCaSS 2023[9]:

- In the lecture "From ROCA (Fun & troubles with RSA keypairs) to improved security certification", Prof. Vashek Matyáš (Masaryk University) provided a brief outline of the core trouble with the Estonian (and Slovak, etc.) eID underlying cryptographic mechanism for electronic signatures. The discussion concluded with suggestions for improving the fragile ecosystem of cybersecurity system certification and security evaluation. In another lecture on "Two lessons from usable security and its experiments", Prof. Vashek Matyáš introduced an interdisciplinary undertaking involving aspects of computer security, psychology and sociology. It explored two particular areas of research - interactions of S/W developers with TLS public-key certificates and the work of developers with two-factor authentication.

[9] The ESSCaSS 2023 lecture material is available at https://courses.cs.ut.ee/t/esscass2023/Main/LectureMaterials

- The ESSCaSS 2023 poster session provided the venue to discuss the recent CHESS research result. Lukáš Daubner (Masaryk University) introduced "Risk-oriented Design for Forensic-Ready Software Systems". Mari Seeba (TÜ arvutiteaduse instituut) presented the "Security Level Evaluation with F4SLE" study. Mariia Bakhtina (University of Tartu) discussed "A Decentralised Public Key Infrastructure for X-Road".
- In a session on Post-quantum Security, the state of the art and challenges in post-quantum cryptography were discussed. In the talk on "Post-quantum Cryptography: Introduction and Current State in Security Protocols", Lukas Malina (Brno University of Technology) overviewed the recent development in security protocols and well-known libraries and their support of quantum-resistant algorithms. In another talk on "Integrating Post-Quantum Cryptography into Existing Systems Today", Petr Muzikant (Cybernetica) considered post-quantum algorithms and how they could be implemented in applications nowadays. In the third talk, Jan Hajny (Brno University of Technology) discussed how post-quantum security could be addressed in Linux encryptors of network traffic.

The 3rd International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), 2023
29 August – 1 September, Italy

The 3rd International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I) at ARES 2023[10] was organised in Benevento, Italy, to discuss ongoing and future research directions in privacy, security, trust, and interdisciplinarity in Intelligent Infrastructures as the Internet of Vehicles, e-Healthcare, Smart Cities services, Smart Grids and Smart Home applications. Co-organised by Lukas Malina (Brno University of Technology), Raimundas Matulevicius (University of Tartu) and Gautam Srivastava (Brandon University), SP2I 2023 featured the keynote talk, six research presentations and a panel discussion.

In the keynote on "Privacy and Verifiability Trade-offs in Voting Systems", Jan Willemson (Cybernetica) explained that complete transparency and verifiability, on the one hand, and privacy to resist coercion attacks, on the other hand, cannot be achieved 100%. The speaker discussed the equilibrium points and highlighted their implications for practical voting systems with the audience.

In the paper "Securing Data Exchange in the Convergence of Metaverse and IoT Applications", Rizwan Patan (Kennesaw State University) introduced the SafeMetaNet approach, which combines proximity-based authentication, encryption, and blockchain technology to establish secure data exchange in the IoT-Metaverse convergence. Another talk, "Data Loss Prevention Solution for Linux Endpoint Devices" by Lukáš Daubner (Masaryk University), overviewed data loss prevention (DLP) approaches in a Linux

[10] https://www.ares-conference.eu/

environment and implementation of a DLP system, demonstrating the chosen viable approaches.
In "Security Level Evaluation with F4SLE", Mari Seeba (University of Tartu, Riigi Infosüsteemi Amet) discussed the Framework for Security Level Evaluation (F4SLE) and the Measurement Application for Self-assessing Security (MASS) tool to explore the security status of organisations and facilitate assessments and supportive data-driven focused interventions at a national level. In the paper "A Decentralised Public Key Infrastructure for X-Road", presented by Raimundas Matulevicius (University of Tartu), an open-access system prototype for an organisation's identity management following self-sovereign identity principles is illustrated in the X-Road use case.

In "On Deploying Quantum-Resistant Cybersecurity in Intelligent Infrastructures", Lukas Malina (Brno University of Technology) presented a practical assessment of some post-quantum cryptography algorithms and discussed how incoming post-quantum migration affects selected areas in intelligent infrastructures. A talk, "On Efficiency and Usability of Group Signatures on Smartphone and Single-board Platforms," by Patrik Dobias (Brno University of Technology), provided an assessment of group signatures on various computing platforms used in modern digital services.

The joint SP2I and ETACS panel presented research, training and collaboration opportunities in CHESS Cyber-Security Excellence Hub challenge areas: Internet of secure things, Security certification, Verification of trustworthy software, Security preservation in blockchain, post-quantum cryptography, Human-centric aspects of cyber-security.

The 4th International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), 2024
30 July 2024, Belgium

The SP2I 2024 workshop aimed to collect the most relevant ongoing research efforts in privacy and security in intelligent infrastructures.

IEEE Estonia section meetup 2024

At the IEEE Estonia Section Meetup 2024, Mubashar Iqbal presented the CHESS project, specifically highlighting CA4. His workshop on blockchain delved into the primary objectives, strategies, and anticipated impacts of CA4 within the broader CHESS initiative, showcasing how blockchain can serve as a critical enabler for enhanced security and risk management.

ETACS Workshop on Education, Training and Awareness in Cybersecurity

Although having significant importance, cybersecurity training and education is not the main topic of many (if any) international conferences or workshops. Therefore, CHESS is participating on the organisation of the Workshop on Education, Training and Awareness in Cybersecurity (ETACS)[11], an annual event focused explicitly on training and education in cybersecurity. In 2023 and 2024, the event was organised by CHESS members as an official CHESS event. The program of ETACS include invited talks, paper presentations, CHESS project description and invitation for collaboration sessions. With 20-40 attendees from not only Europe, but also invited speakers from US and UK, this event significantly improves the visibility and collaboration potential of CHESS in the fields of education, training and awareness raising.

[11] https://www.ares-conference.eu/etacs

Workshop on Process Theory for Security Protocols and Cryptography
18-19 March 2024, Tallinn

An international group of scientists, industry representatives and young researchers gathered in early spring in Tallinn to advance cross-border knowledge exchange on process theory. The workshop was organised by Tallinn University of Technology and aimed to explore the potential of categorical methods in modelling situations that arise in computer security and cryptography. Among the 27 participants were the members of the professional community from the University College London, the University of Pisa, the University of Innsbruck, the University of Oxford, the University of Strathclyde, the University of Padova, the University of Udine, Cybernetica, Input Output (IOHK), Masaryk University and Tallinn University of Technology. It was a great opportunity for the community members to present the latest research output and exchange ideas as well as for the project participants to introduce the CHESS project and raise awareness of our activities.

All of the international workshops presented in Section 3 of this document are included in the following table that depicts all events organised in WP2 of CHESS until and including December 2024. Events that count towards the CHESS KPIs are marked with an asterix.

The events we include in CHESS KPIs 5-8 are only international or cross-regional events organised or co-organised by CHESS targeted at researchers, industries and NGOs and open to wider audiences beyond the CHESS consortium.

Table 5: All events organised within WP2 (until December 2024)

	Name of event	Partners	CA	Acad.	Industry	NGO	Stu.	Other
1	2 MUNI Hacking Days (2023)	MUNI	CA6				83	
2	MUNI Hacking Day December (2023)	MUNI	CA6				43	
3	Online cybersecurity training for students	MUNI	CA6				35	
4	Cybersecurity Summer School 2023	MUNI	CA6				25	
5	Cybersecurity Summer School 2024	MUNI	CA6				30	
6	**Future Cryptography Conference***	RIA, BUT, CYBER	CA5	10	58		2	13
7	**Post-Quantum Cryptography Workshop***	BUT, CYB, MUNI,RIA	CA5 CA1	20	15			17
8	RIA CyberMeetUp	RIA, MUNI	CA4		30			350 online
9	Treshold Workshop	UTARTU, MUNI	CA1 CA4		5		25	
10	Workshop for Estonian Computer Emergency Response Teams	MUNI, RIA	CA2	35	99	120		38
11	InfoSec Seminar	UTARTU, MUNI	CA1	8				
12	3 Privacy Management Seminars	MUNI, BUT, UTARTU	CA1 CA4	21			15	

13	**Mastering Penetration Testing Reports Workshop Tallinn***	CYBER, MUNI	CA6	2	8		1	7
14	**Mastering Penetration Testing Reports Workshop Tartu***	CYBER, MUNI	CA6	3	8			4
15	**Workshop on practical cybersecurity certification***	CYBER, MUNI, RIA	CA2	0	20	5	0	
16	Toolbox presentation (sec-certs) at RIA	RIA, MUNI	CA2	27 participants including people from RIA, University of Tartu and GuardTime				
17	Online workshop for Cybernetica (sec-certs)	CYBER, MUNI	CA2		15			
18	Blockchain workshop at Küberinnovatsioon 2023	UTARTU	CA4	113 researchers, students, industry professionals, governmental organisation				
19	CHESS Industrial Day 2023	MUNI, BUT	CA3	28	15			
20	**The 3rd International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), 2023***	BUT, UTARTU	CA1	25	3	2	5	
21	**The 4th International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), 2024***	UTARTU, BUT	CA1	30	4	3	6	
22	**Workshop on Education, Training and Awareness in Cybersecurity (ETACS 2023)***	BUT, CYBER	CA6	25	5	5	10	
23	**Workshop on Education, Training and Awareness in Cybersecurity (ETACS 2024)***		CA6	15	4	1	5	
24	CHESS workshops at Estonian Summer School in Computer and Systems Science, 2023	UTARTU, MUNI, BUT	CA5 CA2 CA1				120	
25	IEEE Estonia section meetup 2024	UTARTU	CA4	10	5			
26	**Workshop on Process Theory for Security Protocols and Cryptography***	TalTech	CA3	23				
27	BUTCA training for teachers	BUT	CA6 CA5	5				15
28	F4SLE results interpretation seminar included into sectoral infodays	UTARTU, RIA	CA2		110			
29	F4SLE intro included to cybersecurity management training to Climate ministry and Culture ministry subordinate institutions	UTARTU, RIA	CA2		70			
30	Cybersecurity management training for education technologists included F4SLE usage	UTARTU, RIA	CA2		22			

31	Information security standard implementation training day included F4SLE slot	UTARTU, RIA	CA2		120			
32	Exercise Platform – Train the Trainers (2024)	MUNI	CA6	12	4			6
33	Hands-on workshop on cybersecurity training (2024)	MUNI, TalTech	CA6	4				4
34	Online training of national teams European Cybersecurity Challenge (2024)	MUNI	CA6		3	2	60	7
35	CHESS Industrial Day 2024	CYBER, GuardTime	CA3	12	3			
36	Lunch-n-Learn 2024	Redhat, MUNI, BUT	CA3	3	15			
37	PROTECT2024	MUNI	CA3	19	9			23
38	Tabletop training TalTech, Tallinn, 2024	MUNI, TalTech	CA6	2			14	
39	Tabletop training vocational schools, Tallinn, 2024*	MUNI, TalTech	CA6				41	7
	Total number of events:			Acad.	Industry	NGOs	Stu.	Other
	42			**312**	**650**	**143**	**520**	**141**

*These are the events we include in KPIs 5-8, i.e. No. of training/education events organised, No. of trained researchers, users from industry and NGOs.

Table 6: CHESS Key Performance Indicators related to training and knowledge-sharing

KPI No.		Status M24	Aim M24	Aim M48
5	# of Training/education events organised (summer schools, workshops)	10	6	14
6	# of Trained researchers	153	30	120
7	# of Trained users from industry	125	20	80
8	# of Trained users from NGOs	16	15	40

4. Networking and Staff Exchange

As mentioned above, besides organising events, staff exchange and mobility form a second pillar in the CHESS effort on knowledge transfer. In 2024, a series of specialised fellowships were organised within different challenge areas. These fellowships aimed to advance knowledge sharing, find partnerships, and identify collaboration opportunities for ongoing research and practical applications.

Table 6 shows the overall mobility within CHESS in the first 24 months of the project. For privacy reasons, the names of researchers taking part in fellowships have been withheld. Below, we present some of the events and activities these mobilities brought about.

Table 6: Overview of short- and midterm mobilities.

	Who	CA	From	To	Start-end dates
1.	**First Stage Researcher**	CA1, CA4	UTARTU	MUNI, BUT	30 Sep - 19 Oct, 2024
2.	**First Stage Researcher**	CA1, CA4	MUNI	RIA, Tallinn	14-19 May, 2024
				UTARTU	19-31 May, 2024
3.	**First Stage Researcher**	CA1, CA4	MUNI	UTARTU	19-31 May, 2024
				RIA, Tallinn	14-19 May, 2024
4.	**First Stage Researcher**	CA1	MUNI	UTARTU	30 Nov – 16 Dec 2024
5.	**Recognised Researcher**	CA1, CA2	MUNI	UTARTU	1.10.2024 - 1.11.2024; 16.11.2024-14.12.2024
6.	**First Stage Researcher**	CA5	BUT	CYB	1-30 Sept, 2024

University of Tartu (UTARTU) Fellowships

	Who	CA	From	To	Start-end dates
1.	**First Stage Researcher**	CA1, CA4	UTARTU	MUNI, BUT	30 Sep - 19 Oct, 2024

In October 2024, a PhD student from the University of Tartu visited Masaryk University and Brno University of Technology to share her research findings and refine her PhD dissertation with expert feedback from the hosting institutions. Additionally, she aimed to explore potential collaboration opportunities, particularly for postdoctoral research, by familiarising themselves with ongoing studies at these institutions. During the visit, she met with a Professor of Empirical Software Engineering at Paderborn University and a Research Assistant Professor at George Washington University, gaining insights into improving the usability of security tools for developers.

Throughout the stay, she found an opportunity to work with the CRoCS group at MUNI on developing anonymisation-preserving services tailored for blockchain-based systems. Furthermore, her research findings were presented in three different seminars, primarily

conducted within the CHESS project. These are included in Section 3.2, cross-regional knowledge sharing.

Masaryk University (MUNI) Fellowships

	Who	CA	From	To	Start-end dates
2.	**First Stage Researcher**	CA1, CA4	MUNI	RIA, Tallinn	14-19 May, 2024
				UTARTU	19-31 May, 2024
3.	**First Stage Researcher**	CA1, CA4	MUNI	UTARTU	19-31 May, 2024
				RIA, Tallinn	14-19 May, 2024
4.	**First Stage Researcher**	CA1	MUNI	UTARTU	30 Nov – 16 Dec 2024
5.	**Recognised Researcher**	CA1, CA2	MUNI	UTARTU	1.10.2024 - 1.11.2024; 16.11.2024-14.12.2024

We managed to organise all MUNI fellowships thanks to the involvement of our Estonian partners, especially the University of Tartu, which hosted all of the MUNI fellows. All of these fellowships had cross-sectoral character. Even where the official host was UTARTU, the fellows managed to benefit from the close proximity of the university to other CHESS institutions from non-academic sectors (Cybernetica, Guardtime, RIA).

The fellowships aimed to present the results of the CRoCS laboratory in the field of multiparty and threshold cryptography (MPC), attend meetings with industrial partners (in the CHESS project), and continue collaboration with the research team of the University of Tartu based on a joint publication. Also, to develop a collaboration with Cybernetica on two-party ECDSA signature computation on smartcards, which also resulted in a join research paper on the topic.

Two junior researchers (Fellowships No. 2 and 3) spent the first part of their trip to Estonia in Tallinn, where they presented the applied research on threshold cryptography at a meeting of the Estonian RIA institution on 16 May. The presentation was followed by discussions with participants on applications of threshold cryptography. From 19 May to 31 May, they stayed at the University of Tartu and Cybernetica, where they met with researchers from the industry (Guardtime and Cybernetica) to discuss practical use cases in user authentication. On 23 May, they organised a Threshold Cryptography Workshop (see section 3.2) for the University of Tartu students and academic staff, with around 30 attendees. During their fellowship, they also cooperated with researchers from Cybernetica to prepare a prototype of a two-party ECDSA implementation on smartcards. This work resulted in a publication that is now submitted for review.

Another young researcher from MUNI (Fellowship No. 4) stayed in Tartu in December 2024 to present the concept of Adaptive Safety in Autonomous Ecosystems to professor Matulevicius and his group of Requirements Engineering students. This concept utilises a "Social Network" of Autonomous Vehicles and uses traits human-like traits, such as honesty, transparency and trust to improve safety of the whole ecosystem. The students were tasked to utilise a novel method of adjusting existing safety mechanisms of an Autonomous Vehicle to be trust-based. The solutions and the additional data collected from the students will be used to validate the method from the perspective of its correctness and usability. Together with the professor, they started drafting a conference paper that will present the results gained from the data. The paper will be submitted to the ARES conference at the beginning of the year 2025. Furthermore, they attended a cybersecurity meetup in Tallinn organised by RIA.

A recognised researcher from MUNI went to the University of Tartu to collaborate with the Information Security group led by Prof. Raimundas Matulevičius on joint research in forensic-ready, privacy-preserving vehicle sharing (Fellowship No.5). The main challenge is to find a balance between the privacy and forensic readiness goals to ensure an acceptable level of privacy preservation of the vehicle-sharing service users while allowing for investigation of security and business-related incidents (e.g., service misuse, and insider attacks). The planned results are a conference and a journal paper, which are still being written and will be part of the dissemination report.

During his stay, he gave one presentation on the ongoing research on InfoSec seminar to 8 people. The gathered feedback on the topic of forensic-ready, privacy-preserving vehicle sharing and intermediate results feed back into this researcher's current work. He also spoke at a short offensive security training for the Information Security group members. Additionally, he met and discussed possible research collaborations with members of the Information Security group members and other cybersecurity experts in Estonia. Other points of contact were members of Cybernetica with whom future collaborations were discussed. To make the most of this fellowship, he attended the RIA CyberMeetUp, organised by the Estonian Information System Authority, held in Tallinn, the Ethics of AI seminar by EXAI, and several institute seminars on HPC. The fellowship enabled him to share expertise in forensic readiness and offensive security with the team. On the other hand, the expertise within the Information Security group on privacy-preserving technologies, security standards, and requirements engineering

will be an asset for future work. Thus, the fellowship provided a perfect match for the research topic. As for future cooperation, he first outlined several follow-up research directions, branching from the topic of forensic-ready, privacy-preserving vehicle sharing. Furthermore, he discussed opportunities for several security-related projects and university courses. Most importantly, this shorter stay has led to his application for an open Research Fellow position at the University of Tartu to continue working at the institute. This should allow for deepening knowledge-sharing and provide opportunities for realising the discussed future endeavours.

Brno University of Technology (BUT) Fellowships

	Who	CA	From	To	Start-end dates
6.	**First Stage Researcher**	CA5	BUT	CYB	1-30 Sept, 2024

Organising fellowships and student/staff exchange is an integral part of the education and training process. As CA5 is a rather small group, organising longer visits is a more complicated task. Nevertheless, one fellowship and one Czech - Estonian employee transfer have been successfully realised in the period of 2023 - 2024. These CA5 members have gained international experience thanks to the CHESS project.

A BUT student took an internship at Cybernetica, Estonia for 1 month in 2024. The purpose of the visit was to establish and evaluate a post-quantum connection between Estonia and Czechia. The internship was successfully completed and report from activities is available at both institutions

Also, a former BUT student has been employed by Cybernetica, Estonia, working on the CA5 activities since 2023. He has participated significantly in most CA5 activities, including publication and presentation activities.

We had planned to have ten fellowships in the first two years. Six of these have been carried out in 2024. Two fellowships were postponed till next year. Two visits of MUNI senior researchers to Estonia had to be shortened and thus do not fall under fellowships. However, they form the basis for future collaboration and planned fellowships in the next year.

5. Training Materials

CHESS training and awareness raising events have produced and presented an array of publications and material. While all presentations can be found on the official CHESS website[12] and are subject to the general dissemination report, some of the infrastructure and material used in teaching and training events described in Section 3 is openly available and could be used in future trainings. As CHESS aims to reach a broad audience, we strive to make most material openly accessible and want to share best practices in cybersecurity education.

In order to attain knowledge and hand-on experience we appreciate practical approaches and labs. These include cyber range platforms such as the **KYPO Cyber Range Platform**[13], a KYPO training facility at Masaryk University that has been used during several CHESS events, mainly in CA6. The KYPO Cyber Range Platform is open-source software and is a unique state-of-the-art solution for creating, conducting, and evaluating cybersecurity hands-on training. Another valuable platform provided by MUNI is the **INJECT Exercise Platform**[14], designed for the preparation, execution, and evaluation of tabletop exercises focused on managing cybersecurity crises and responding to incidents that threaten critical information infrastructure. Developed in close collaboration with NÚKIB, it has been integrated into the curriculum at the Faculty of Informatics at MUNI. The INJECT platform offers a dynamic approach to cybersecurity training and is currently being used in the CHESS project to engage early adopters in the Czech Republic and Estonia.

During a recent training for trainers, namely secondary school teachers in the Czech Republic, the cyber range platform **BUTCA[15], Brno University of Technology's Cyber Arena** was employed among others.

[12] https://chess-eu.cs.ut.ee/publications/
[13] https://crp.kypo.muni.cz/
[14] https://inject.muni.cz/
[15] BUTCA - KYBERNETICKÁ ARÉNA | Ústav telekomunikací

Specifically for the purpose of CA5, some advanced infrastructures have been used. While the technology is usually financed from other resources (mostly national), the **CHESS CA5** members have direct access to the infrastructure and can do research and experimental verification using it. In particular, the network infrastructure for the evaluation of Czech – Estonian post-quantum secure channel has been established and used in the CHESS project by students from both regions. This infrastructure is depicted in Figure 1.

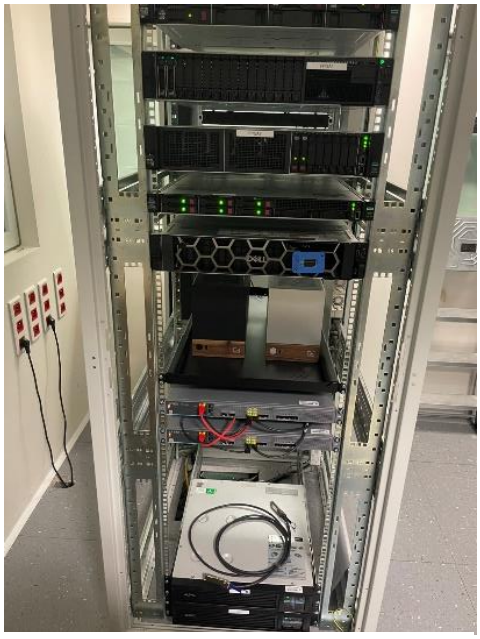


Figure 1: Infrastructure at BUT used for CA5 activities.

To support CA4 activities under the CHESS project, a range of documentation has been developed, including detailed reports, educational materials, and thesis reports. These materials enhance training sessions, workshops, and conferences by providing insights into blockchain security, risk management, and emerging cryptographic approaches. These reports and materials are accessible from CHESS's official website[16].

With regards to training on Security Certification the **workshops on F4SLE** used material that is publicly available with the MASS data collection tool[17].

All official CHESS events have presentations publicly available on the CHESS webpage[18].

[16] https://chess-eu.cs.ut.ee/presentations/ and https://chess-eu.cs.ut.ee/reseach-areas/security-preservation-in-blockchain/

[17] https://mass.cloud.ut.ee/massui/#/

[18] https://chess-eu.cs.ut.ee/presentations/.

6. Planned Activities

Many of the events outlined in Section 3 are planned to be continued in the next year to expand on the success and use momentum to create a lasting effect and outreach for CHESS. For example, in 2025, there are already multiple post-quantum workshops co-organised in CA5 with national cybersecurity authorities. We also plan cybersecurity training and education workshop ETACS and events for educatores and students. The continuation of workshops such as ETACS or the 5th International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), in CA1 and CA4 allows recurring contact with researchers and experts in cybersecurity from various sectors.

Having successfully carried out fellowships in 2023 and 2024, we acknowledge the need to increase Czech – Estonian collaboration by promoting staff exchange within the consortium and will focus on this aspect in the next period. Several researchers, including senior researchers from both South Moravia and Estonia, plan their fellowships in 2025. As part of CA4, we have several key activities planned. One of the major initiatives is a fellowship program in Brno, where we will host two targeted workshops on blockchain at Brno University of Technology (BUT) and Masaryk University (MUNI). These workshops aim to strengthen collaborative knowledge transfer and engage participants in discussions on blockchain security advancements.

Another recurring event, the CHESS Cybersecurity Summer School (2025) (CA6) will be organised for the finalists of the national Kybersoutez.cz competition. The event will feature a CTF Jeopardy, Active/Defense CTF, and a tabletop exercise.

In addition to introducing the INJECT platform to TalTech project partners as part of the CHESS hands-on workshop on cybersecurity training, we have received mutual feedback on how to proceed with the project, how the INJECT platform works, and what needs to be done for the next steps. The next step is to collaboratively develop a tabletop exercise that can be used on the INJECT platform. Also, we received positive feedback from the Train the Trainers workshops for experts in the field of tabletops. Participants expressed great interest in the topic and are especially looking to innovate the tabletop format by transitioning from traditional pen-and-paper methods to using dedicated software to prepare and deliver tabletops.

The success of such interactive training and education events held already in CHESS has motivated us to increase these formats. So, we are planning to organise tabletop trainings and tabletop train the trainers events for students, industry professionals, and other participants, addressing attendees from both the South Moravia region and Estonia.

In addition, our team is committed to continuously disseminating research outcomes through presentations at various conferences and events. This ensures our work, e.g. on blockchain's security potential, reaches a broad academic and industry audience. By sharing our findings, we aim to further stimulate dialogue and development around blockchain-enabled security solutions within the European Union and beyond, supporting CHESS's mission of cybersecurity advancement across sectors.

Regarding Security Certification (CA2) we plan Training on regulatory frameworks (Czech, EU) for cybersecurity certification. Moreover, we will analysing the Common Criteria and FIPS certification documents using sec-certs. Also, we will host a training for Future Cryptography 2025: Reliable Cryptography with a focus on certification.

A closer look at the training plans for all challenge areas revealed that there is a general interest in providing soft skill training dealing with public speaking and presenting, training for junior researchers on proposal writing or PR skills to acquire knowledge on how to broaden the outreach for scientific results. This sentiment was reflected in *D1.1 Training and knowledge transfer needs and opportunities (SWOT) in the selected areas in South Moravia and Estonia*. Therefore, we are planning to incorporate a workshop for junior researchers on transferal skills in a cybersecurity setting.

7. Conclusions

Training and education events in CHESS have had a wide outreach with participants from the public and private sector joining seminars, workshops and industrial days in the two regions of Estonia and South Moravia and beyond. Some of these activities have been held in the past two years with growing numbers of attendees.

The actual number of events and outreach exceeded our expectations and shows the value of training and education events in the realm of cybersecurity, as all six involved challenge areas have used the various event formats to raise awareness, present practical solutions and engage with the scientific community, companies and the wider public.

The activities, training events and conferences planned for 2025 will continue the efforts CHESS has shown so far and will be expanded by e.g. trainings of transferal skills for cybersecurity researchers.

All in all, the audience reached through CHESS training and awareness-raising events spans the industry, national security agencies, academia, and the civil sector. Some collaborations and networking efforts have resulted in new proposed collaborations on future projects that are still in the application process.