CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

D4.1
Dissemination, Exploitation and Communication Plan

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	D4.1
Deliverable name	Dissemination, Exploitation and Communication Plan
Lead Beneficiary	Masaryk University
Type	R — Document, report
Dissemination Level	PU - Public
Work Package No	WP4
Due Date	June 2023
Date	30 June 2023
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

- Raimundas Matulevičius (UTARTU)

Contributors

- Antonin Kucera (MUNI)
- Jan Hajny (BUT)
- Liina Kamm (CYBER)
- Lukas Malina (BUT)
- Raimundas Matulevičius (UTARTU)
- Vashek Matyas (MUNI)
- Zuzana Vemolova (MUNI)

Reviewers

- Zuzana Vemolova (MUNI)
- Vashek Matyas (MUNI)

CHESS Consortium

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

Abbreviations

CA – challenge area
CHESS – Cyber-security Excellence Hub in Estonia and South Moravia
ICT – information and communication technology
KPI – key performance indicator
NGO – non-governmental organisation
OA – open access
R&I – research and innovation
TA – target audience
WP – work package

Executive Summary

This document provides a detailed CHESS Dissemination, Exploitation and Communication Plan. It describes the objectives, target audience, and strategic activities and links them with the CHESS key performance indicators. The document also explains the actions and instruments for communication, dissemination, and exploitation. It presents a project logo, presentation templates, reports and deliverables, project brochures and posters. The document also discusses monitoring. In the end, it highlights the following activities.

Table of Contents

List of Tables

List of Figures

1 Introduction

CHESS is the Cyber-security Excellence Hub in Estonia and South Moravia. Its main objectives [1] are to

- Develop a cross-border joint cybersecurity research and innovation (R&I) strategy aligned with Czechia's and Estonia's smart specialisation strategies,
- Propose action and investment plans for implementation of the strategy in six challenge areas of cybersecurity (i.e., internet of secure things, security certification, verification of trustworthy software, security preservation in blockchain technology, post-quantum cryptography, and human-centric security),
- Initiate at least 12 small-scale R&I projects consolidating academia business linkages to demonstrate the validity of ideas and provide evidence to obtain additional investments,
- Develop a training strategy for both regions to increase cross-border/sectoral cooperation and increase needed skills around the six challenge areas, and
- Raise visibility, citizen engagement, technology transfer, entrepreneurship training, staff exchange, mutual learning, etc.

The project must have an explicitly defined communication, dissemination, and exploitation plan to support achieving the CHESS objectives. The project's Grant Agreement includes the basic plan for communication (*inform, promote and communicate project activities and results*), dissemination (*open science, knowledge and result*) and exploitation (*knowledge and results for others to use; concrete use of results*). The purpose of this document is to outline the **detailed strategy, specific actions and instruments** which would set up and describe the **infrastructure** for project communication dissemination and exploitation.

The document is structured as follows: in Section 2, the objectives, target audience, and strategy of communication, dissemination, and exploitation are introduced. Section 3 overviews the actions, and Section 4 presents the communication, dissemination, and exploitation instruments. Section 5 discusses monitoring. Finally, Section 6 summarises and concludes the report.

2 Objectives, Target Audience and Strategy

In this section, first, the objectives of communication, dissemination and exploitation are discussed. Next, it defines the target audience and illustrates the relationship between the target audience and objectives. Further, the section discusses the strategy for achieving the objectives by performing different communication, dissemination, and exploitation activities. The section also illustrates the link between the communication, dissemination and exploitation objectives and the CHESS deliverables.

2.1 Objectives

Communication and dissemination should help reach the CHESS project's objectives. It should contribute to awareness, participation, and involvement.

It is necessary to maintain **awareness** about a joint cross-border cybersecurity R&I strategy aligned with South Moravia and Estonia's smart specialization strategies, action and investment plans for implementing this strategy its six cybersecurity focus areas. The CHESS project also aims to raise visibility, citizen engagement, technology transfer, entrepreneurship training, staff exchange, mutual learning, etc.

Action and investment plans for implementing the strategy in the six challenge areas of cybersecurity and initialising small-scale R&I projects consolidating academia business linkages to demonstrate the validity of ideas and provide evidence to obtain additional investments will require active **participation**. CHESS will invite companies and citizens of Estonia and South Moravia to participate in the CHESS workshops and training seminars.

A training strategy for both regions to increase cross-border/sectoral cooperation and increase needed skills around the six priority areas will result in the **involvement** of international networks of experts from different sectors. Potentially this would attract community contributions to the organized scientific and training workshops.

The following four communication, dissemination, and exploitation objectives are defined:

O1: Share research results and build an international and regional reputation.
O2: Invite to collaborate and support the uptake of R&I results.
O3: Provide training and awareness about project results.
O4: Inform about project activities and achievements and engage citizens and the societal sector.

2.2 Target Audience

To strengthen the cybersecurity ecosystem in both regions and disseminate the project results, we have carefully selected the target audience. The audience includes:

- **TA1: Academic community**: cybersecurity and ICT researchers; and more specifically, researchers in the fields of security certification, Internet of (Secure) Things, verification of trustworthy software, blockchain, post-quantum cryptography, as well as human-centric aspects of cybersecurity.

- **TA2: Companies.** These companies provide cybersecurity solutions in ICT, blockchain, and (post-) quantum cryptography in CHESS regions and beyond. This also includes spin-offs and emerging entrepreneurs.
- **TA3: Policy-makers and public authorities** dealing with state/EU data and computer systems, digital infrastructures, and cyber defence.
- **TA4: General public and NGOs** in the field of cybersecurity/ data protection

Using different messages, content, and channels for different target audiences is essential to achieve the dissemination goals. Table 1 summarises the relationship among the target audience, dissemination goals, dissemination contents and channels.

Table 1: Relationship Among TA, Objectives, Contents, and Channels

Target audience	Objective	Contents	Dissemination channels
TA1: Academic community	**O1:** Share research results. **O2:** Invite to collaborate. **O4:** Inform about project activities and achievements.	• Scientific publications • Research presentations/ posters • Demonstrations • Project brochure • Project poster	• Scientific journals, • Scientific conferences and workshops • Public events and workshops and forums • Project website
TA2: Companies	**O1:** Share research results. **O2:** Invite to collaborate. **O3:** Provide training and awareness.	• Demonstrations • MSc thesis • Project deliverables • Training material	• Training workshops/ schools • Project demonstrations • Partners' website • Project website
TA3: Policy-makers and public authorities	**O1:** Share research results. **O3:** Provide training and awareness. **O4:** Inform about project activities and achievements.	• Research presentations/ posters • Demonstrations • Project deliverables • Training material • Newsletter • Project brochure • Project poster	• Project demonstrations • Training workshops and training schools • Public events and workshops and forums • Partners' website • Project website
TA4: General public and NGOs	**O3:** Provide training and awareness. **O4:** Inform about project activities and achievements.	• Training material, • Newsletters, • Project brochure; • Project poster	• Training workshops and training schools • Public events and workshops and forums • Partners' website • Project website

For instance, to achieve O1, O2, and O4, the **academic community** (TA1) should receive messages about the advances of CHESS partners in challenge areas and identify avenues for future research and advanced training opportunities offered by CHESS for academics from outside the consortium. Hence CHESS participating universities are excellent destinations for researchers, post-doctoral and doctoral students. CHESS will inform

companies (TA2) will be informed about how the CHESS results can improve commercial services. Here CHESS should offer support to regional actors in cybersecurity and ICT. It should settle potential avenues for further research and cooperation. To achieve O1, O3, and O4, the **policymakers and public authorities** (T3) should receive messages about CHESS research results. The CHESS partners will explain how to ensure the safety and smooth operation of European digital society and protect EU digital infrastructures against potential cyber-attacks. The project aims to raise awareness among the **general public and NGOs** (T4) about the risks in cyberspace. It should help relevant NGOs integrate CHESS results into their activities and build cooperation to promote cyber risk awareness.

Potentially different target audiences will form networks both at the national and European levels, including governmental institutions (national/EU), EC Agencies, and other European projects. Table 2 lists networks, organisations and projects for CHESS communication, dissemination, and exploitation activities.

2.3 Strategy

Table 3 lists strategic activities to achieve CHESS communication, dissemination, and exploitation objectives. Regarding communication, the CHESS project partners will announce accepted papers and conference/workshop talks on social media channels. Partners will present scientific results at international conferences and workshops. CHESS will communicate information about published article on CHESS Website. The partners will promote the organised scientific and training workshops/seminars and other events on social media. Partners will share information about the events in newsletters and publish on the CHESS and partner organisational websites.

Regarding dissemination, the CHESS partners will publish articles and papers at international venues, including journals, conferences, and workshops. They will organise scientific workshops at international venues and publish their proceedings with recognised publishers. Partners will organise seminars, regional workshops, and training schools for the Estonian and South Moravian companies to present research results. At the events, partners will disseminate information about the project through brochures, posters, and presentations. The project deliverables will be shared using the CHESS website.

Regarding exploitation, the CHESS project will share the results, deliverables, and scientific and training presentations through the CHESS website. Project partners will publish the research article and papers using the open-access principles. CHESS will invite regional and international partners to collaborate in the research activities and submit new project proposals. Partners will try to transfer research results to practical use (create prototypes, software, and demonstrations). The partners will provide training seminars and workshops to teach the citizens and societal sector to apply the project outcomes in daily activities.

Table 2: CHESS Targeted Networks/Organisations

Name	Country/ region/ type	Website
Network Security Monitoring Cluster	Czech Republic	https://www.nsmcluster.com/en/
CESNET	Czech Republic	https://www.cesnet.cz/
Estonian Information System's Authority (RIA), • CERT-EE/CSIRT • Cyber4Dev • CyberNET • NCSC-EE	Estonia	https://www.ria.ee/ https://cyber4dev.eu https://www.eucybernet.eu/
Cyber defence unit of the Defence League	Estonia	https://www.kaitseliit.ee/en/cyber-unit
International Centre for Defence and Security	Estonia	https://icds.ee/
Association of Information Technology and Telecommunications	Estonia	https://itl.ee/en/
Foundation CR14	Estonia	https://cr14.ee/
Estonian Defence Forces Cyber Command	Estonia	https://mil.ee/en/landforces/cyber-command/
Startup Estonia	Estonia	https://startupestonia.ee/focus-areas/cybertech
ISACA Estonia Chapter	Estonia	https://www.eisay.ee
eGovernment Academy: National Cyber Security Index	Estonia	https://ncsi.ega.ee
European Cybersecurity Competence Centre (ECCC)	EU	https://cybersecurity-centre.europa.eu/
European Cyber Security Organisation (ECSO)	EU	https://ecs-org.eu
European Network and Information Security Agency (ENISA)	EU	https://www.enisa.europa.eu
SOCCER: Developing and deploying SOC capabilities for the academic sector - a teamwork of Universities and RTOs in the CEE region (call: DIGITAL-ECCC-2022-CYBER-03)	EU project	
CHAISE: Blockchain skills for Europe (grand No: 621646-EPP-1-2020-1-FR-EPPKA2-SSA-B)	EU project, ERASMUS+ program	https://chaise-blockchainskills.eu

Table 3: Strategic Activities to Achieve Objectives

Objectives	Communication	Dissemination	Exploitation
O1: Disseminate research results and build the international and regional reputation	Present at international conferences and workshops. Announce about accepted papers, about conference/workshop talks on social media (Facebook, LinkedIn, Twitter, YouTube). Announce about published paper on CHESS website.	Publish at international venues– journals, conferences, workshops.	Publish the conference presentations on CHESS website. Supervised, defended CHESS Master thesis on small-scale project topics both in Estonia and South Moravia. Articles and papers published using open access principles in the recognised venues. Submit new research proposals.
	Promote the organised scientific workshops on social media. Write newsletters about the organised events, publish on the CHESS website (and partners' websites).	Organise scientific workshops at international venues. Publish scientific workshop proceeding with recognised publishers. Organise seminars, regional workshops, training schools for the Estonian and South Moravian companies to present research results.	
O2: Invite to collaborate and support the uptake of R&I results;	Promote the organised scientific workshops on social media. Write newsletters about the organised scientific events, publish on the CHESS website (and partners' websites).	Organise scientific workshops at international venues. Publish scientific workshop proceeding with recognised publishers. Organise seminars, regional workshops, training schools for the Estonian and South Moravian companies to present research results.	Invite regional and international partners to collaborate in the research activities. Submit new project proposals. Transfer research results to practical use (create prototypes, software, demonstrations). Research outputs used in companies.

O3: Provide training and awareness about project results;	Promote training workshops and seminars on social media. Write newsletters about the organised training events, publish on the CHESS website (and partners' websites).	Organise seminars, regional workshops, training schools for Estonia and South Moravia.	Share training presentations openly on the CHESS website. Trained participants would apply the gained knowledge in their daily activities.
O4: Inform about project activities and achievements and engage citizens and the societal sector.	Write newsletters about the CHESS events and achievements, publish on the CHESS website (and partners websites).	Participate in public events, disseminate brochures, posters. Share the project deliverables using the CHESS website.	Citizens and societal sector would apply the project results in their daily activities.

2.4 Contribution to Project Objectives

CHESS will produce several project deliverables, and hence the communication, dissemination, and exploitation support the TA regarding awareness, participation, and involvement. Table 4 explains the link between the CHESS deliverables and dissemination and communication activities.

Table 4: Communication and Dissemination Support to CHESS Deliverables

WP	CHESS deliverables	Dissemination and communication
WP1	D1.1. Training and knowledge transfer needs and opportunities (SWOT) in the selected areas in South Moravia and Estonia	Invite the regional stakeholders to share their needs for training and knowledge transfer in the field of cybersecurity.
	D1.2. Strategy for Cross-Regional Collaboration in Cybersecurity	Communicate and invite the cross-regional stakeholders to collaborate on training and research activities.
	D1.3 Action Plans for 6 CHESS Challenge Research Areas	Promote and support awareness of the research activities in the six selected challenge areas. Organise scientific workshops in relevant international venues. Co-author and publish research results in international venues (including journals, conferences, and workshops).
	D1.4 Roadmap for Cross-Regional Collaboration in Cybersecurity	Disseminate the roadmap to relevant networks at national and European levels. Disseminate and promote the roadmap to the cross-regional stakeholders.
WP2	D2.1 Mid-term Report on Training and Mobility	Promote training and knowledge transfer events and possible mobility plan in selected areas in South Moravia and Estonia. Communicate activities to invite learners to participate in the training and knowledge transfer activities.
	D2.2 Final Report on Training and Mobility	Communicate the report on training and mobility to relevant networks at national and European levels. Disseminate and promote the report on training and mobility to the cross-regional stakeholders.
WP3	D3.1 Mid-term evaluation report of CHESS R&I activities	Promote the research report to the international and regional stakeholders, including the companies, the public sector, etc.
	D3.2 Report on engagement of the ecosystems into CHESS R&I	Communicate to the regional stakeholders and invite them to collaborate in the research activities.
	D3.3 Final evaluation of CHESS R&I activities	Communicate the CHESS R&I report to relevant networks at national and European levels. Disseminate and promote the CHESS R&I report to the cross-regional stakeholders.
WP5	D5.1 Risk Management Plan	Communicate the risk management plan to the project partners. Publish the risk management plan in the CHESS communication channels.

	D5.2 Initial Data Management Plan	Communicate the risk management plan to the project partners. Publish the risk management plan in the CHESS communication channels.

3 Actions

This section presents actions for communication, dissemination, and exploitation. The CHESS partners will publish the research results in international venues (i.e., journals and magazines) to disseminate research results and build an international reputation. In addition, the partners will publish and participate in international scientific events (conferences and workshops). They will disseminate project outcomes by organising international and national workshops, training schools, and public events. These organised events will help to invite (both academic and industrial partners) to collaborate and inform about project activities and achievements.

While publishing the articles and papers, the partners will be committed to open science principles. The open science practices will include:

- Open access (OA) to publications.
- Early open sharing of research (including presentations and training material).
- Encouraging reproducibility of research outputs.

More information on data management can be found in D5.2 CHESS Data Management Plan [2].

3.1 Publishing CHESS Research Results

CHESS will conduct research in small-scale projects in all six challenge areas. The project partners will target international journals and magazines to disseminate CHESS research results and build an international reputation. Table 5 provides a sample of the target journals and magazines.

Table 5: Journals and Magazines for Publishing Scientific Results

Journal / Magazine	Publisher	Website
Computers & Security (**COSE**)	Elsevier Ltd.	https://www.sciencedirect.com/journal/computers-and-security
Journal of Information Security and Applications (**JISA**)	Elsevier Ltd.	https://www.sciencedirect.com/journal/journal-of-information-security-and-applications
Computer Standards & Interfaces (**CS&I**)	Elsevier Ltd.	https://www.sciencedirect.com/journal/computer-standards-and-interfaces
Computer Networks	Elsevier Ltd.	https://www.sciencedirect.com/journal/computer-networks
International Journal of Information Security (**IJIS**)	Springer	https://www.springer.com/journal/10207
Journal of Cryptographic Engineering	Springer	https://www.springer.com/journal/13389/
IEEE Security and Privacy	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
IEEE Transactions on forensics and security	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
IEEE Sensors Journal	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=7361
PeerJ Computer Science	PeerJ	https://peerj.com/computer-science/

To disseminate research results and build an international reputation, to invite collaboration and support the uptake of R&I results, the CHESS partners will write and publish scientific papers in conferences and workshops internationally and regionally. Table 6 lists several venues which the project partners will target.

Table 6: Conferences to Submit and Publish the CHESS Scientific Results

Conference (workshop)	International/ regional	Timing	Website
International Conference on Availability, Reliability and Security (**ARES**)	International	Annual	https://www.ares-conference.eu
International Baltic Conference on Digital Business and Intelligent Systems (**Baltic DB&IS**)	International, with regional focus	Biannual	https://dbis2022.lu.lv
International Conference on Advanced Information Systems Engineering (**CAiSE**)	International	Annual	https://caise23.svit.usj.es
European Symposium on Research in Computer Security (**ESORICS**)	International	Annual	https://esorics2023.org/#about
International Congress on Ultra Modern Telecommunications and Control Systems (**ICUMT**)	International	Annual	https://icumt.info/2023/
Joint International Conference on Artificial Intelligence (**IJCAI**)	International	Annual	https://ijcai-23.org/
Nordic Conference on Secure IT Systems (**NordSec**)	International	Annual	https://uni.oslomet.no/nordsec2023/
Research Challenges in Information Science (**RCIS**)	International	Annual	https://www.rcis-conf.com/rcis2023/
International Conference on Theory and Applications of Satisfiability Testing (**SAT**)	International	Annual	http://satisfiability.org/SAT23/
International Conference on Security and Cryptography (**SECRYPT**)	International	Annual	https://secrypt.scitevents.org
International Symposium on Foundations & Practice of Security (**FPS**)	International	Annual	https://www.fps-2023.com/

3.2 Organising CHESS Events, and Training Events

To invite regional and international scientific communities to collaborate on CHESS activities, the partners will organise scientific workshops at well-recognised international conferences. Table 7 lists a few CHESS-associated workshops that CHESS partners plan to organise.

Table 7: Workshops Organised by the CHESS Partners

CHESS-associated workshop	Venue	Primary CHESS challenge area	Timing
International Workshop on Security and Privacy in Intelligent Infrastructures (**SP2I**)	ARES	CA1, CA2, CA4, CA5	Annually
Industrial Day		CA3	Annually
Workshop on Education, Training and Awareness in Cybersecurity (**ETACS**)	ARES	CA5, CA6	Annually

To provide training and awareness about CHESS results, the CHESS project partners will provide training workshops, seminars, and lectures. Partners will also participate in public events to inform about the project's activities and achievements and engage citizens and the societal sector. Table 8 presents a sample of venues for training schools, workshops, and public events for CHESS dissemination.

In WP1, Task 1.1. Mapping the Ecosystem Needs and Opportunities, SPARTA will prepare a SWOT analysis, i.e., D1.1 Training and knowledge transfer needs and opportunities in the selected South Moravia and Estonia areas. One of the mapping results will be the list of relevant stakeholders we wish to collaborate with, including relevant networks, projects, and various initiatives. This mapping exercise will help us specify/broaden the target audience of our communication activities.

Table 8: Training Schools, Workshops, and Public Events for CHESS Dissemination

CHESS-related event	Country	Timing	Website
Brno Security Meetings	Czech Republic	Twice a year	https://www.vut.cz/www_base/vutdisk.php?i=315171a0ec
DevConf	Czech Republic	Annual	https://www.devconf.info/cz/
Estonian Summer School on Computer and Systems Science (**ESSCaSS**)	Estonia	Annual	https://courses.cs.ut.ee/t/esscass2023/
Hacking Day	Czech Republic	Annual	
Information Security Summit (**IS2**)	Czech Republic	Annual	https://is2.cz/
International Summer School on Program Analysis and Verification	Estonia	Annual	
Küberinnovatsioon	Estonia	Annual	https://kuberinnovatsioon.cs.ut.ee
Santa's Crypto Get-Together	Czech Republic	Annual	https://mkb.tns.cz/index.short.html.en

3.3 CHESS Final Dissemination Workshops

During the last year (M36-M48), the CHESS project will organise two final dissemination workshops. UTARTU will organise one workshop in Estonia and MUNI – in South Moravia. The final workshops will combine dissemination and training activities, address the global expert audience, and highlight the expertise of both South Moravian and Estonian region in the target cybersecurity areas (e.g., Internet of Safe Things, Security Certification, Verification of Trustworthy Software, Security Preservation in Blockchain Technology, Post-Quantum Cryptography, and Human Centric Aspects of Security).

3.4 Partners' Contribution to Communication and Dissemination

Table 9 illustrates how CHESS partners will contribute to the communication and dissemination activities.

Table 9: Partners' Contribution to Dissemination and Communication

CHESS partners	Activities
Universities (MUNI, UTARTU, BRNO, TalTech)	• Co-author and publish scientific publications (articles and papers) at the international journal, conferences, and workshops. • Organise training schools and seminars. • Publish press releases (newsletters) on their websites. • Disseminate project dissemination material (brochures, posters) at events, conferences, workshops, training schools, etc.). • Identify potential users of the project results and inform them about the project activities. • Disseminate results through social media, announce about the events, training schools.
Companies (Cybernetica, Guardtime, RedHat)	• Participate in the co-authored publications for international journals, conferences, and workshops. • Exploit their market leadership positions to disseminate the project results in sponsored workshops, to customers, business partners and within national and international security associations. • Disseminate results through social media, share information about the events and training schools. • Disseminate project dissemination material (brochures, posters) at events, conferences, workshops, training schools, etc)
Public Agency (RIA), **NGO** (CSH), **Associated Partners** (NCISA, JIC, EISA)	• Provide annual cybersecurity assessment reports with overviews of incidents and cybersecurity services. • Disseminate project dissemination material (brochures, posters) at events. • Disseminate results through social media, and share information about the events and training schools. • Disseminate project dissemination material (brochures, posters) at events, conferences, workshops, training schools, etc.). • Inform about project activities and achievements and engage citizens and the societal sector.

4 Instruments

This section presents the instruments used to communicate, disseminate, and exploit CHESS results. It includes a description of the identity brand, the project website, social media channels, newsletters, and promotion tools.

4.1 Identity Brand

Figure 1 illustrates the **logo** of the CHESS project. Different colour schemes can be used/ adapted depending on the partners' preferences. The logo is used in the project presentations (see Figure 2), website, social media channels, deliverables (e.g., this document), brochure, poster, and any other instrument used to communicate CHESS activities, events and results to the target community.

Black/white *Blue background* *Blue/black/white*

Figure 1: CHESS Project Logo

Figure 2: The CHESS Presentation Template

4.2 Website

The CHESS website (see Figure 3, URL: ***https://chess-eu.cs.ut.ee***) is the primary interface for communicating and disseminating the project's objectives, activities, and results to the target audiences. It will also overview the partnership, and main project results, including deliverables, publications, and other outputs, which will become available for the target audience later for the exploitation activities. The project will use the CHESS website to *communicate* information about the published articles and papers, inform about the organised events (including regional and international), and invite the target audience to the training seminars and workshops. The project's website will *disseminate* the CHESS publications, training material, deliverables, and demonstrations. Since the material is available through the website, the target audience can *exploit* it for its purposes. The CHESS website introduces the project structure, challenge areas, training, and awareness activities. The project website will be further described in the accompanying document D4.2.

Figure 3: Landing Page of CHESS Project's Website

4.3 Social Media

The CHESS project will use social media channels to reach different target audiences, communicate the upcoming events (regional and international workshops, public events, training schools), and disseminate the project news and results. Understanding that different target audiences overlap and potentially use various social media channels is also essential. CHESS partners will use the following:

- Twitter (see Figure 4): https://twitter.com/CHESS_EU
- Facebook (see Figure 5): https://www.facebook.com/ChessExcellenceHub
- LinkedIn (see Figure 6): https://www.linkedin.com/company/chess-cyber-security-excellence-hub/
- YouTube (see Figure 7): https://www.youtube.com/channel/UCjuwIAQobUL7kQWBgb36y7Q

Figure 4: CHESS Twitter Landing Page

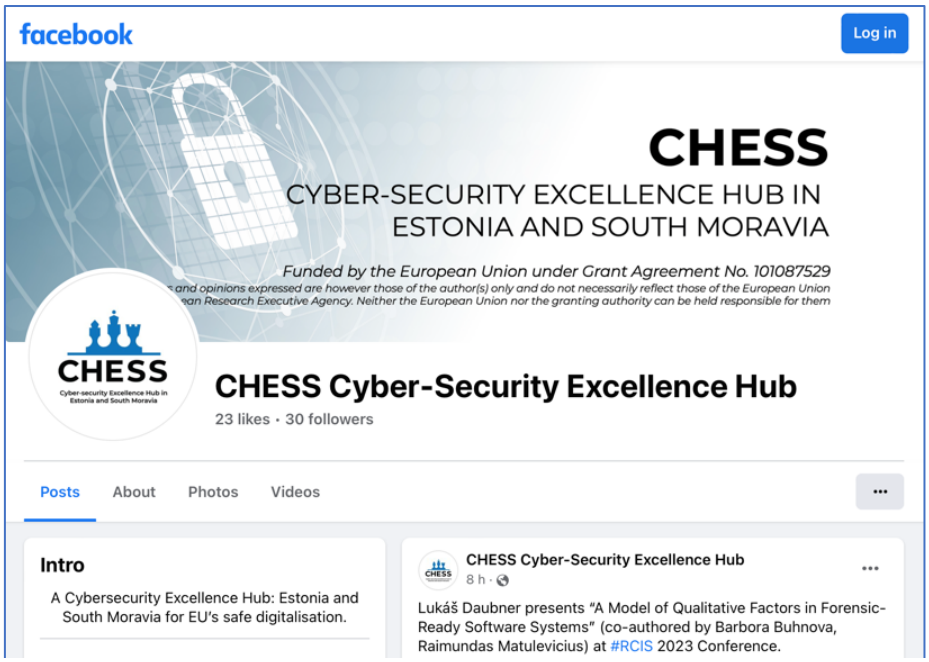

Figure 5: CHESS Facebook Landing Page

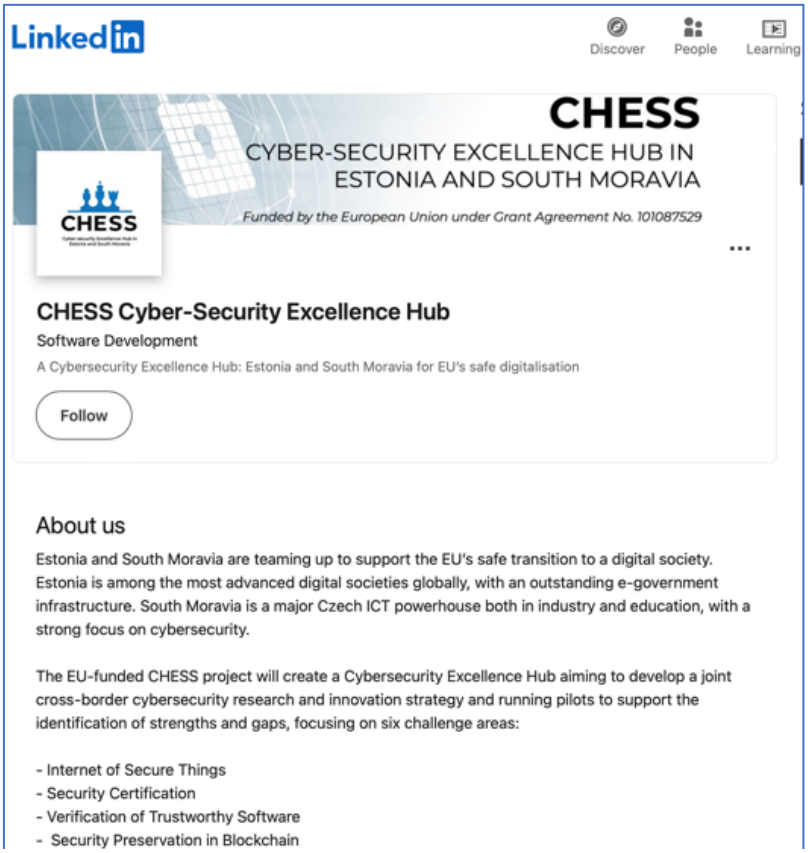

Figure 6: CHESS LinkedIn Landing Page

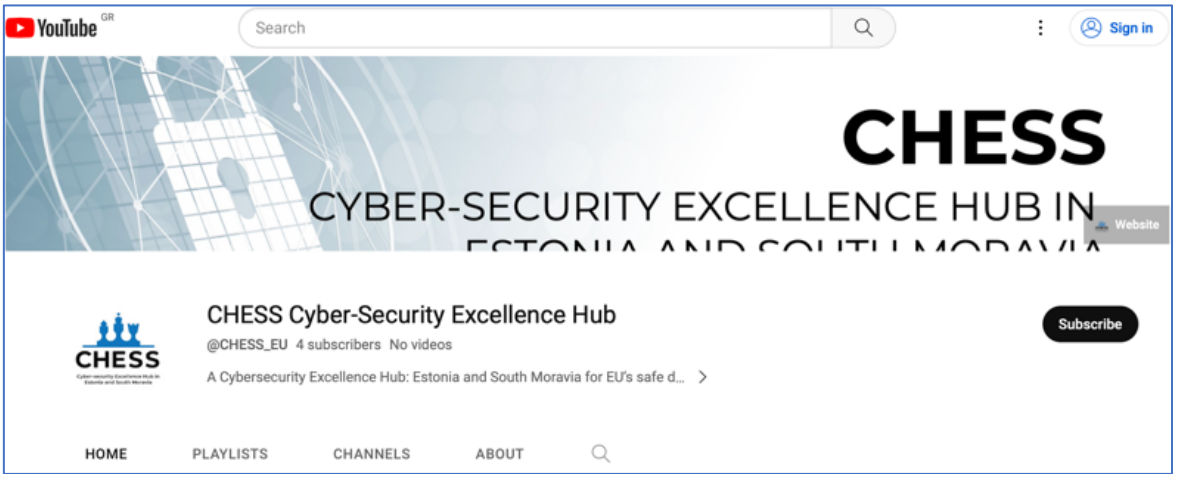

Figure 7: CHESS YouTube Landing Page

4.4 Newsletters

The newsletter is the instrument to communicate the news about the events (both regional and international) that the CHESS partners organise. The project will publish the newsletters on the CHESS website, and partners will republish them on the organisational websites.

4.5 Promotion Instruments

In the CHESS project, we create promotional instruments, such as CHESS brochures and CHESS posters. Both will include brief information about the project goals, timeline, involved partners, etc. Partners will distribute brochures and posters to the target audiences during the CHESS events in the exhibition areas. These will be a good tool for presenting the project's objectives and activities.

5 Monitoring

In this section we discuss how communication, dissemination, and exploitation activities are monitored and evaluated. Table 10 illustrates the metrics to estimate the performance of the used communication and dissemination instruments.

Table 10: Metrics to Count the Performance of CHESS Instruments

Instrument		Metrics
Website		Unique visitors, number of visitors, Pages, Hits, Bandwidth
Social media	Twitter	Impression, Engagement, Engagement rate
	LinkedIn	Visitors, visitor demographics (job function, top industry)
	Facebook	Number of website likes, number of followers, post reach, post engagement
	YouTube	Number of videos (demonstrators/ videos)
Newsletters		Number of newsletters, their reachability (number of readers)
CHESS posters/ brochures		Number of posters/ brochures distributed

Table 11 illustrates the link between the CHESS key performance indicators and the objectives of communication, dissemination, and exploitation. The table provides the estimates for the M24, M48, for 4 and 10 years after the project completion [1].

Table 11: Link Between the Objectives and KPIs

Objectives	CHESS key performance indicators	M24	M48	4 years after	10 years after
O1: Share research results	**KPI1:** Number of scientific papers in cybersecurity / in high-impact journals (co-) authored by teams from the CHESS regions	6/2	16/6	42/16	90/35
	KPI2: Number of – CHESS deliverables delivered	6	14	n/a	n/a
	KPI3: Number of open-source implementations	2	8	18	36
	KPI4: Number of final student theses based on cross-helix cooperation (cybersecurity topics in collaboration with industry or another sector)	5	30	50	100
	KPI5: Number of deployment of technologies/systems/methods cross-helix (between sectors)	0	10	15	30
	KPI6: Number of deployment of technologies/systems/methods cross-regions	0	6	10	15
O2: Invite collaborate	**KPI7:** Number of joint R&I proposals	1	5	10	18
	KPI8: Number of cybersecurity researchers moving between South Moravia and Estonia	10	20	40	80
	KPI9: Increase in the number of international staff (average across universities/businesses)	0%	3%	4%	5%
O3: Provide training and awareness	**KPI10:** Number of training/education events organized (summer schools, workshops)	6	14	30	60
	KPI11: Number of trained researchers	30	120	300	500
	KPI12: Number of trained users from industry	20	80	150	280
	KPI13: Number of trained users from NGOs	15	40	90	200
O4: Inform about project activities and achievements	**KPI14:** Number of attendees to awareness-raising and communication events	100	500	1200	2000
	KPI15: Number of CHESS-enabled cybersecurity start-ups/spin-offs	0	2	6	12

6 Concluding Remarks and Next Steps

This deliverable presents the communication, dissemination, and exploitation plan. After defining the objective, overviewing the target audience and strategic activities, this report describes the communication, dissemination and exploitation actions and instruments and discusses monitoring.

The following communication, dissemination and exploitation tasks consist of the continuous implementation, monitoring and updating (as necessary) of the dissemination, exploitation, and communication plan. The project partners will monitor the plan's implementation and prepare intermediate and final dissemination and communications reports. The partners will continuously update the plan based on the project's progress. Project partners will create dedicated mailing lists, prepare press-releases, and give interviews to promote our research.

The project will continue maintenance of website and social media accounts. These will include all information about the project, partners and our events and results. We will explore integrating the website as a subdomain or section of UTARTU existing websites to ensure accessibility. All partners will promote the project on their websites & social media.

We also start promoting the deployment and commercialization of CHESS results through regional innovation ecosystem support. The project will engage ecosystem interfaces involved as beneficiaries (RIA, CSH), associated partners (NCISA, JIC), and supporting entities (EAS) in provision of a comprehensive support system to innovators, spin-offs, and emerging entrepreneurs. Regional start-up competitions, incubation spaces, business consultancy services, and entrepreneurship training will be promoted to the CHESS community and the broader cybersecurity R&I ecosystem in South Moravia and Estonia.

All partners will communicate to expert audience and increase their awareness of the cross-regional strength represented in CHESS. CHESS plans to promote joint attendance to research conferences. Also, given the inclusion of R&I activities in the CHESS project, we will seek to publish papers in scientific journals. We will organize dedicated dissemination workshops with potential user groups for deployment-ready results. Where appropriate, we will prepare press-releases and give interviews to promote our research. We will organize workshops, lectures and seminars engaging the public in cybersecurity R&I. Some will have a awareness-raising component, making the audience more perceptive of the risks they face in cyberspace. Others will be focused on popularization, building passion for science.

Deliverable D4.3 on *Materials from workshops and dissemination events* will be prepared at the end of the project by M48.

References

[1] CHESS Project Proposal, 2022

[2] CHESS: Initial Data Management Plan, June 2023. Available at: https://chess-eu.cs.ut.ee/results/deliverables/

Annexes

Annexes to this deliverable are not public and are shared only within the consortium.
Annexes are:

- Annex 1: Means for the Intra-Communication.
  It includes the project mailing lists used for the different purposes available to all project partners.

- Annex 2: Monitoring tools.
  It includes templates for internal reporting of different project activities, including dissemination and communication actions. It details instructions and guidance on what not to forget when e.g., organising a CHESS event or training, disseminate or communicate their activities or travel within the project.

- Annex 3: Acknowledgement of EU funding.