CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

D4.1
Dissemination, Exploitation and Communication Plan Update

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 Update
Lead Beneficiary	Masaryk University
Type	R – Document, report
Dissemination Level	PU – Public
Work Package No	WP4
Initial Plan submitted	30 June 2023
Update submitted	
Version	2

Funded by the European Union

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

Editor

- 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)

History of Changes

Page / Section	Nature of change and reason
p. 4	CHESS Consortium: Estonian Information Security Authority (associated) is substituted with the Estonian Association of Information Technology and Telecommunications (associated).
p. 6	Executive Summary: Updated according to the recent changes in the current document.
p. 7	Table of Contents: Updated according to the recent changes in the current document.
p. 8	List of Tables: Updated according to the recent changes in the current document. Table 10 is removed. New tables 10 to 22 are added. Table 12 is now Table 23
p. 8	List of Figures: Updated according to the recent changes in the current document. Figures 8 to 13 are added.
p. 9 / Section 1	Introduction: The paragraph describing the structure of the deliverable is updated according to the changes in the current document.
p. 13	Table 2 is updated with a few new networks and organisations.
p. 17	Table 5 is updated with new entries of journals and magazines for publishing scientific results.
p. 18	Table 6 is updated with new entries for conferences to submit and publish the CHESS scientific results.
p. 19	Table 7 is updated with new entries for organised workshops and conferences by the CHESS partners.
p. 20	Table 9: In line for “Public Agency, NGO, and Associated Partners: removed EISA, added ITL
p. 23 / Section 4.3	Figures 4, 5, 6 and 7 have been updated.
p. 27 / Section 4.4	Section 4.4 is complemented with a few additional information on the targets of the newsletters. Figure 8 is added.
p. 30 / Section 5	Section 5 is entirely rewritten: • The previous table on metrics to count the performance of CHESS instruments is removed. • Subsections “5.1. Monitoring the CHESS Website”, “5.2. Monitoring CHESS X Social Media Channel”, “5.3. Monitoring CHESS Facebook Social Media Channel”, “5.4. Monitoring CHESS LinkedIn Social Media Channel”, and “5.5. Monitoring CHESS YouTube Channel are added. • In each of the subsections, the metrics for monitoring the communication, dissemination, and exploitation activities are defined. The illustrative examples of the metric performance are given. • Subsection “5.6. Link between the Objectives and KPI” illustrates the achievement of which KPI contribute to the achievement of which objectives.
p. 43 / Section 6	The new section on dissemination and exploitation activities has been added.
p. 45 / Section 7	The previous Section 6 is renumbered to Section 7. Its context is updated according to the recent changes in the current document.

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 Association of Information Technology and Telecommunications (associated)	ITL	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 how the performance of the project's instruments (e.g., the CHESS website and social media channels) is monitored.

This is the second version of the CHESS Dissemination, Exploitation and Communication Plan. In comparison to the first version, which was produced at the beginning of the CHESS project (30.06.2023), this document explicitly highlights the metrics used to evaluate the communication and dissemination activities. The report illustrates the successful use of the CHESS project's website and social media channels for communication and dissemination, and it lays the basis for the exploitation activities in terms of using the project results for continuing research, training, education and outreach. Additionally, this document provides several dissemination and exploitation activities to be performed after the CHESS project is over.

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 communication plan (*inform, promote and communicate project activities and results*), dissemination (*open science, knowledge and results*) and exploitation (*knowledge and results for others to use; concrete use of results*). The purpose of this document is to outline the **detailed strategy, specifications, and instruments that** 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 metrics and presents some examples of the performance of the CHESS website and the social media channels. Section 6 discusses dissemination and exploitation activities after the CHESS project is over. Finally, Section 7 summarises and concludes this deliverable.

2 Objectives, Target Audience and Strategy

In this section, the objectives of communication, dissemination, and exploitation are discussed first. 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 specialisation strategies and action and investment plans for implementing this strategy in 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. This would attract community contributions to the organised 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

We have carefully selected the target audience to strengthen the cybersecurity ecosystem in both regions and disseminate the project results. 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) 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 the European digital society and protect EU digital infrastructures against potential cyberattacks. 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 the published article on the 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 the 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	https://soccer.agh.edu.pl/en/
CHAISE: Blockchain skills for Europe (grand No: 621646-EPP-1-2020-1-FR-EPPKA2-SSA-B)	EU project, ERASMUS+ program	https://chaise-blockchainskills.eu
CYBERCHALLENGE: Challenges Solving in Cybersecurity Study Program	EU project, ERASMUS+ program	https://www.cyberchallenge-erasmus.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 in 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; 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 the 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
Journal of Education and Information Technologies	Springer	https://link.springer.com/journal/10639
Complex Systems Informatics and Modeling Quarterly (CSIMQ)	RTU Press	https://csimq-journals.rtu.lv/csimq
IEEE Access	IEEE	https://ieeeaccess.ieee.org/
PeerJ Computer Science	PeerJ	https://peerj.com/computer-science/
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
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
Computer Networks	Elsevier Ltd.	https://www.sciencedirect.com/journal/computer-networks

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)	Acronym	Website
International Conference on Security and Cryptography	SECRYPT	https://secrypt.scitevents.org
International Symposium on Foundations & Practice of Security	FPS	https://www.fps-2023.com/
International Conference on Availability, Reliability and Security	ARES	https://www.ares-conference.eu/
Nordic Conference on Secure IT Systems	NordSec	https://uni.oslomet.no/nordsec2023/
International Conference on Historical Cryptology	HistoCrypt	https://histocrypt.org/past/2024/page/2/
International Conference on Information Systems Engineering	CAiSE	https://caise-conference.diag.uniroma1.it/
Research Challenges in Information Science	RCIS	https://www.rcis-conf.com/rcis2025/
International Joint Conference on Artificial Intelligence (IJCAI)	IJCAI	https://www.ijcai.org/
AAAI Conference on Artificial Intelligence	AAAI	https://aaai.org/conference/aaai/
International Conference on Theory and Applications of Satisfiability Testing	SAT	https://www.satisfiability.org/
International Conference on Tools and Algorithms for the Construction and Analysis of Systems	TACAS	https://tacas.info/
International Symposium on Mathematical Foundations of Computer Science	MFCS	https://mfcs2025.mimuw.edu.pl/
International Conference on Foundations of Software Science and Computation Structures	FoSSaCS	https://etaps.org/2025/conferences/fossacs/
Smart Card Research and Advanced Application Conference	CARDIS	https://cardis.org/
The Technical Symposium on Computer Science Education	SIGCSE TS	https://sigcse2025.sigcse.org/
International Conference on Business Informatics Research	BIR	https://bir2025.rtu.lv/

International Conference on Perspectives in Business Informatics	Baltic DB&IS	https://dbis2026.cs.ut.ee/
Practices of Enterprise Modelling	PoEM	https://poem2025.unige.ch/

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/Conferences 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
Nordic Conference on Secure IT Systems (**NordSec**)		CA1, CA2, CA3, CA4, CA5, CA6	Annual
International Baltic Conference on Digital Business and Intelligent Systems (**Baltic DB&IS**)		CA1, CA2, CA3, CA4, CA5, CA6	Biannual
Future Cryptography Conference		CA1, CA2, CA3, CA4, CA5, CA6	Annual

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 a 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, ITL)	• 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 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 provide an overview of the partnership and main project results, including deliverables, publications, and other outputs, which will become available for the target audience later for exploitation activities. The project will use the CHESS website to *communicate* information about published articles and papers, inform about organised events (regional and international), and invite the target audience to 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 their 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.

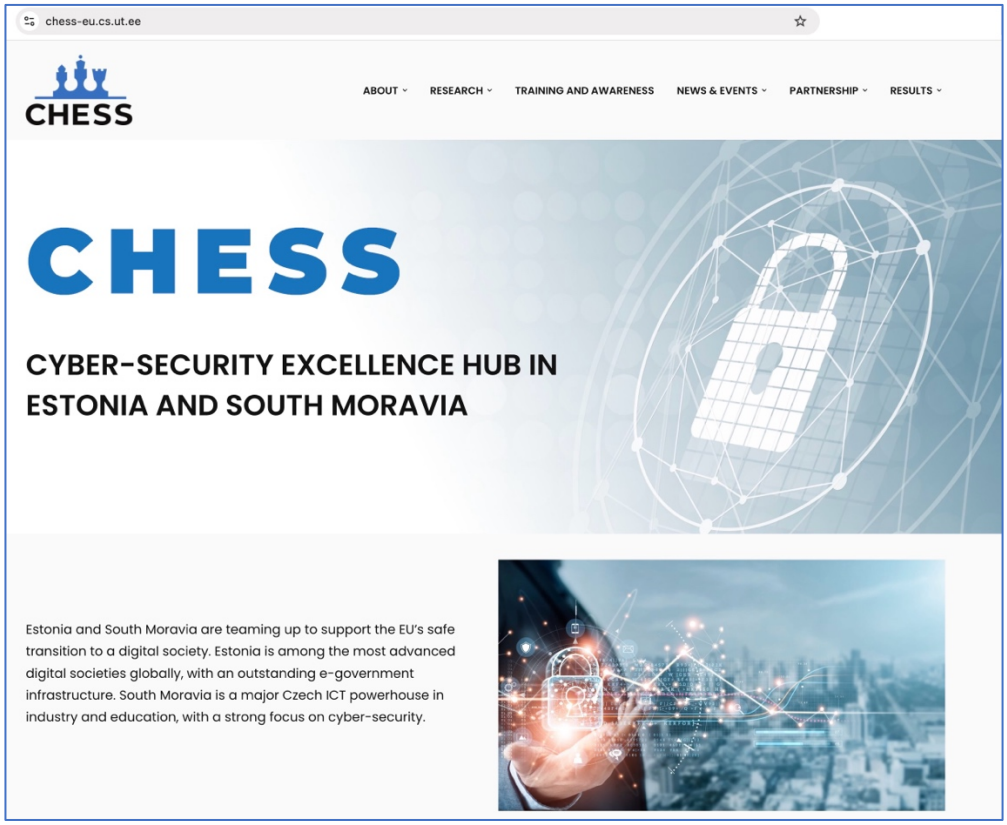


Figure 3: Landing Page of CHESS Project's Website

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 X Landing Page

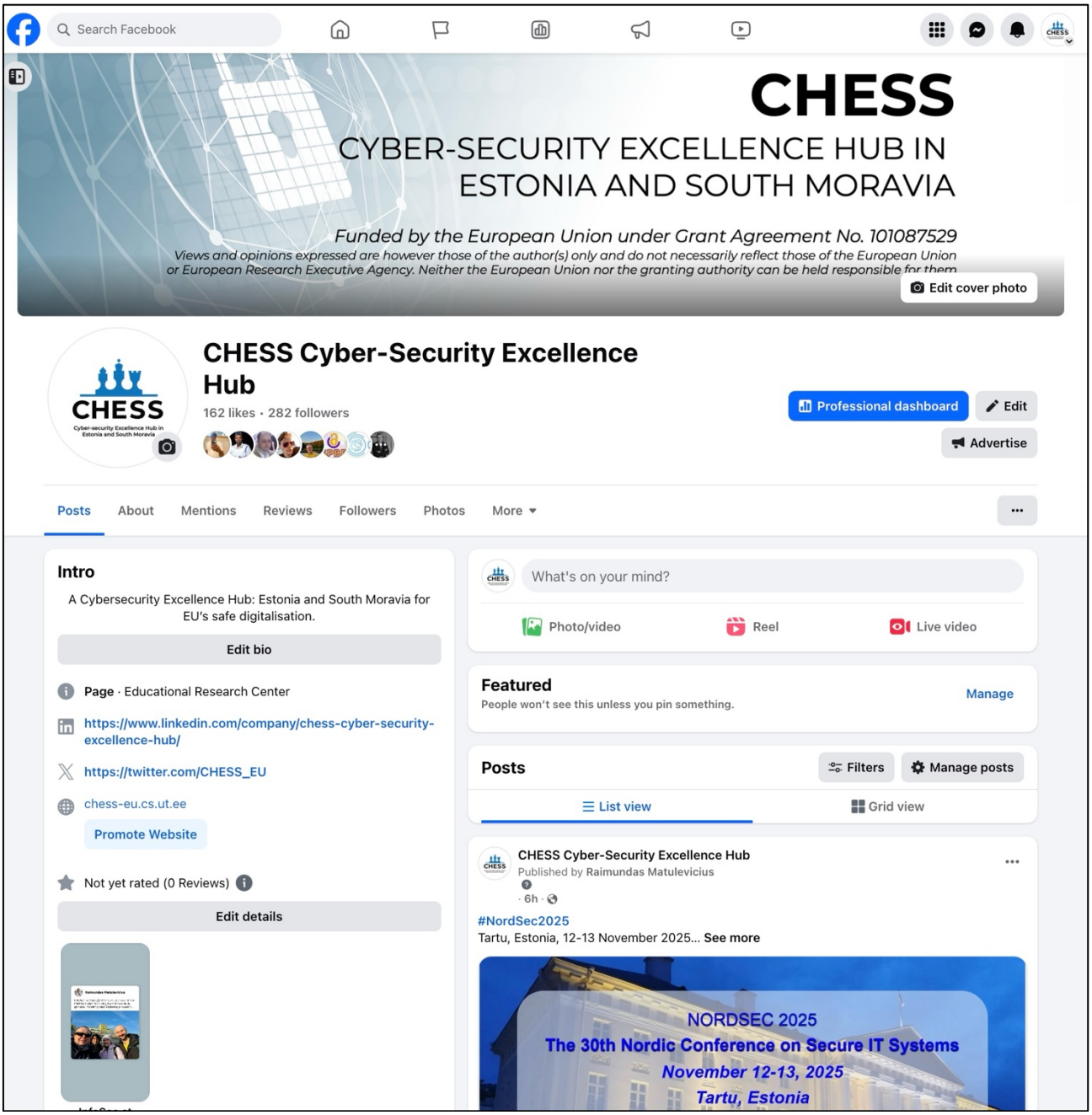


Figure 5: CHESS Facebook Landing Page

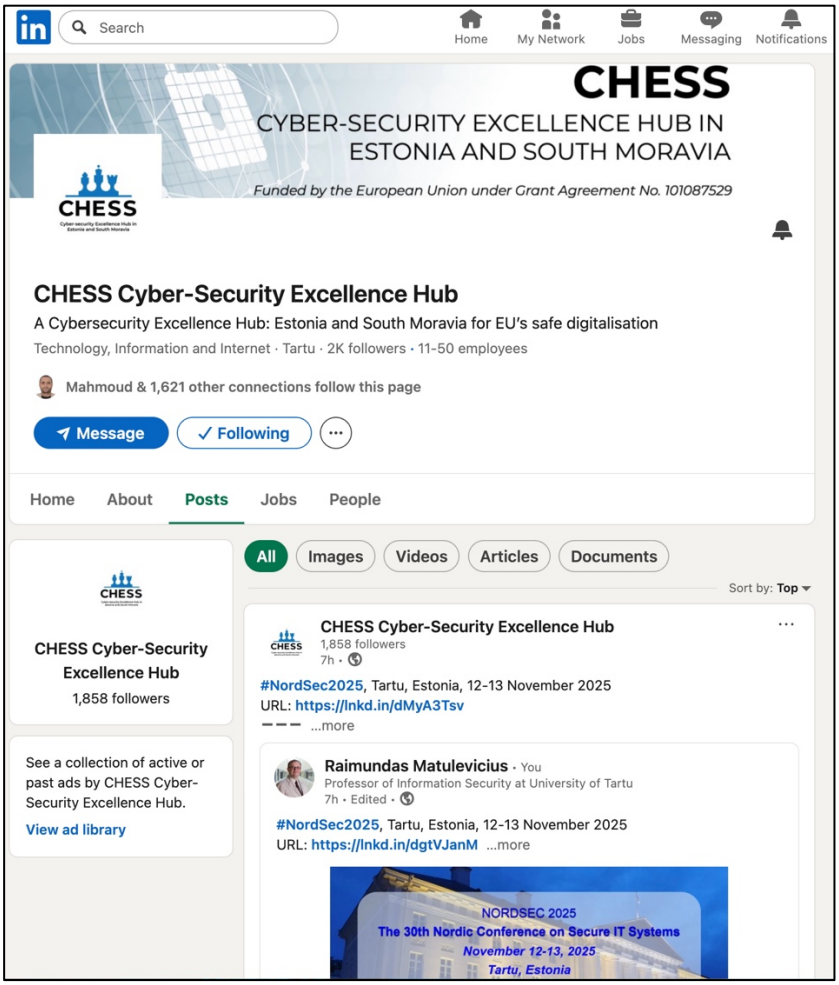


Figure 6: CHESS LinkedIn Landing Page

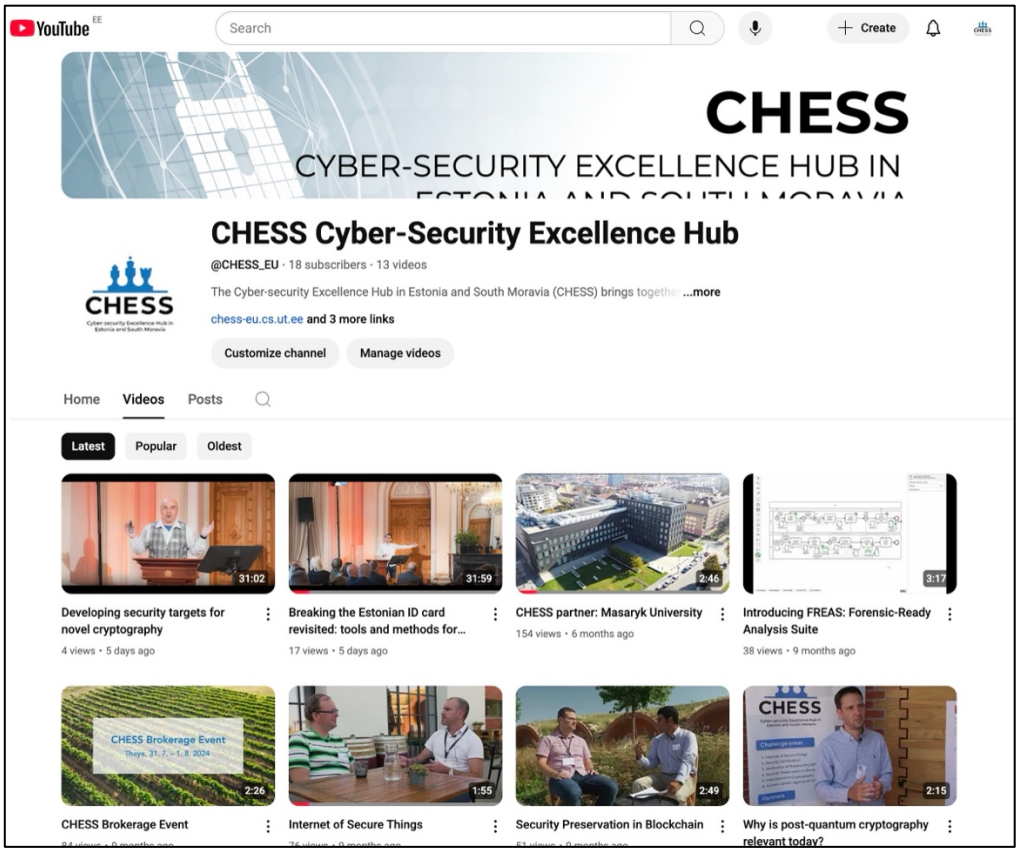


Figure 7: CHESS YouTube Landing Page

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 (see Figure 8), and partners will republish them on the organisational websites. The news includes short reports about the CHESS events (e.g., "Future Cryptography Conference 2025 in Tallinn"), CHESS fellowships (e.g., "Research Fellowship of Martin Macak from the Masaryk University"), CHESS follow-up research projects (e.g., "Big Success for CHESS"), changes in the CHESS consortium (*"Estonian Association of Information Technology and Telecommunications (ITL) joining CHESS*"), and other.

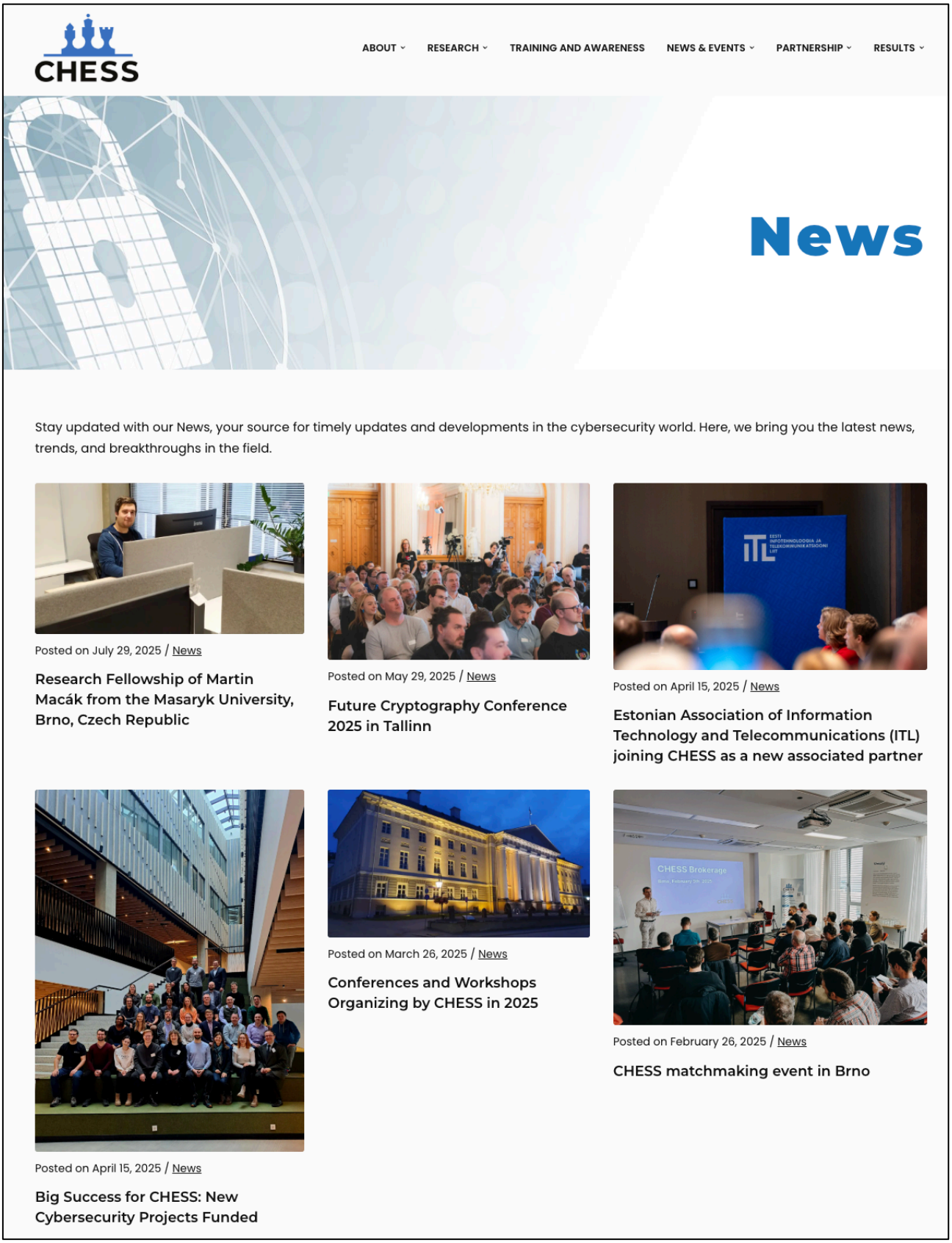


Figure 8: CHESS Newsletter Site

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

This section discusses how communication, dissemination, and exploitation activities are monitored and evaluated. We will monitor the CHESS website (https://chess-eu.cs.ut.ee) and social media channels.

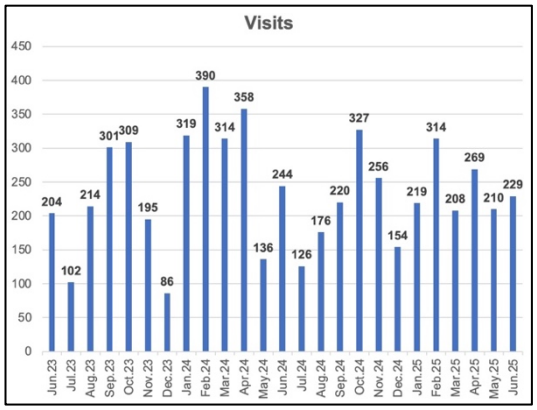
- X: https://x.com/CHESS_EU
- Facebook: https://www.facebook.com/ChessExcellenceHub
- LinkedIn: https://www.linkedin.com/company/chess-cyber-security-excellence-hub/
- YouTube: https://www.youtube.com/channel/UCjuwIAQobUL7kQWBgb36y7Q

5.1 Monitoring the CHESS Website

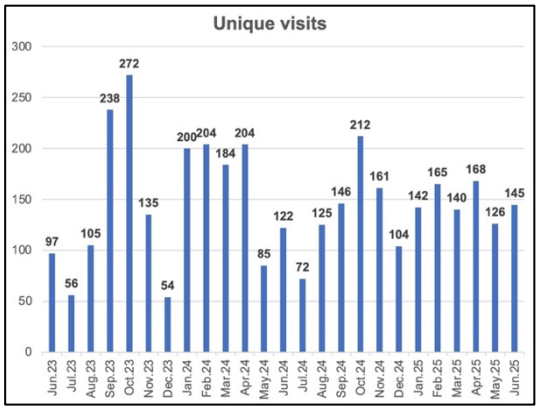
The CHESS website is monitored using the Matomo Analytics - Ethical Stats [3]. The metrics are defined in Table 10. In Figure 9, the performance of the CHESS website is illustrated using Visits (a), Unique visits (b), Average visit duration (secs) (c), Pageviews (d), Unique pageviews (e), Actions per visit (f), Maximum actions in one visit (g), and Downloads (h) metrics.

Table 10: CHESS Website Performance Metrics

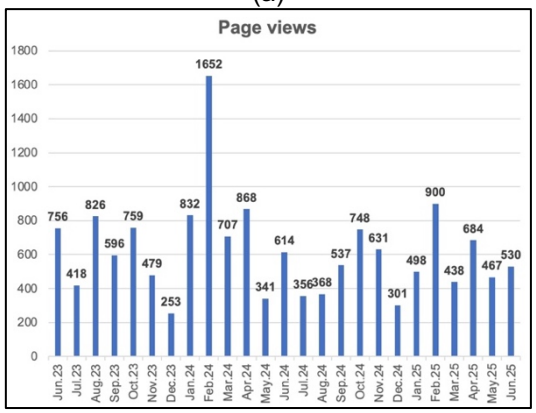
Metrics	Definition
Visits	"Visit" represents a session of user activity on a website defined by a series of interactions within a specific timeframe. The metric helps to explain user engagement and website performance. A visit ends after a period of inactivity or when a new campaign is initiated.
Unique visits	"Unique visit" represents an individual user who visits a website within a specific time frame, regardless of how many times they access the site during that period.
Average visit duration (secs)	"Average visit duration" measures the average amount of time visitors spend on the website during a single visit (or session). It's calculated by dividing the total time spent by all visitors by the number of visits.
Pageviews	"Pageviews" represent the total number of times a specific page on a website has been viewed or loaded.
Unique pageviews	"Unique pageviews" represent a number of sessions during which a specific page was viewed at least once, regardless of how many times it was viewed within that session. It provides a measure of how many distinct visitors have interacted with a particular page.
Actions per visit	"Actions per visit" refers to the average number of interactions a visitor has with your website during a single visit. These interactions are page views, downloads, clicks on links (both internal and external), and site searches.
Maximum actions in one visit	"Maximum actions on one visit" refers to the highest number of actions (like page views, downloads, or events) recorded within a single user session on the website. It helps understand how engaged visitors are interacting with the website.
Downloads	"Downloads" refer to the number of times files (PDFs, documents, and media) have been downloaded from the website.



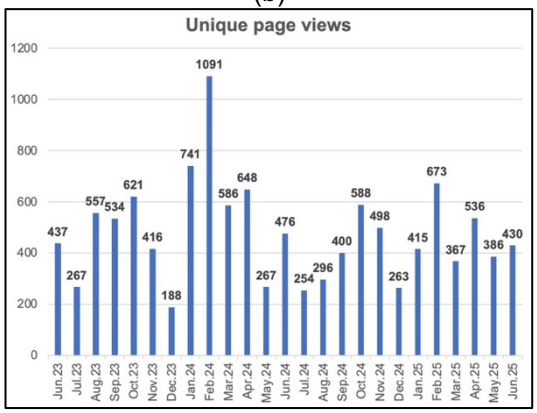
(a)



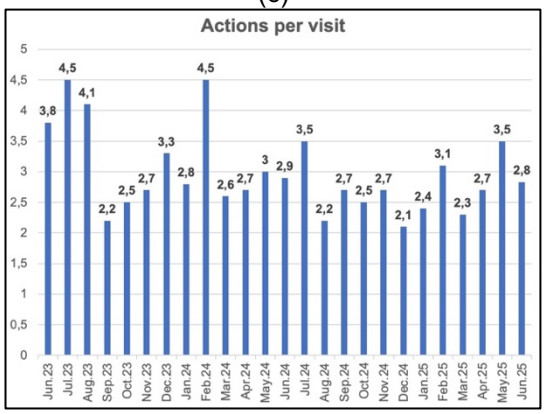
(b)



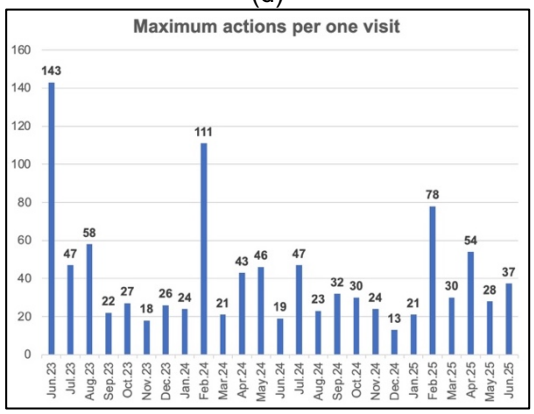
(c)



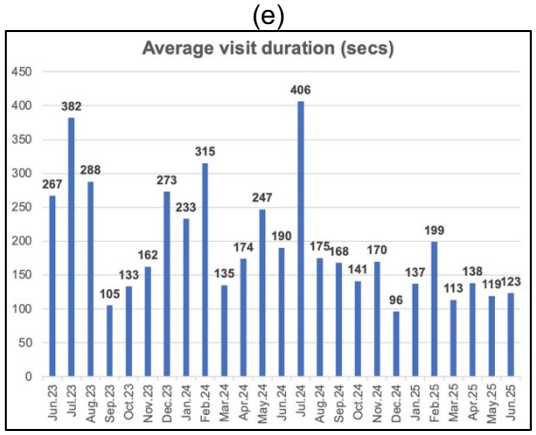
(d)



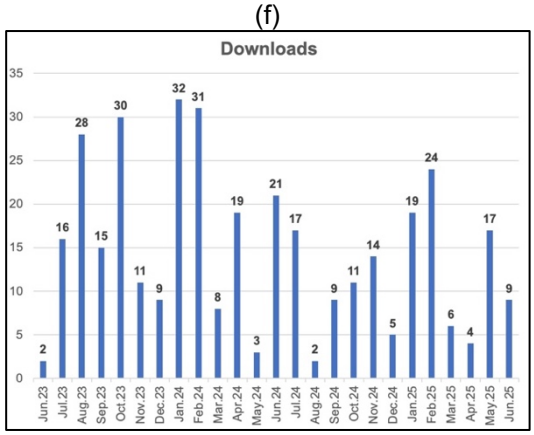
(e)



(f)



(g)



(h)

Figure 9: Performance of the CHESS Website

Table 11 provides a summary of the CHESS website performance since the beginning of opening the project's website till the 30th of June 2025. The table presents both average performance per month and the total measurement of the performance during this period.

Table 11: Summary of the CHESS Website Performance

Metric	Average per month	Total
Visits	235,2	5880
Unique visits	146,5	3662
Average visit duration (secs)	195,6	
Pageviews	622,3	15559
Unique pageviews	477,4	11935
Actions per visit	2,97	74
Maximum actions in one visit	40,9	
Downloads	14,48	362

5.2 Monitoring CHESS X Social Media Channel

The CHESS X social media channel is at https://x.com/CHESS_EU. Its performance is measured using metrics listed in Table 12. This table also includes explanations of the metrics adapted from the X social media.

Table 12: Performance Metrics of CHESS X Social Media Channel

Metric	Explanation
Impressions	"Impressions" – times the posts were seen on X
Engagement rate (%)	"Engagement rate" – post engagements divided by impressions.
Engagement	"Engagement" – the number of times your content was engaged with.
Posts	"Posts" – the number of times your content was posted.
Repost	"Repost" – number of times your posts were reposted
Likes	"Likes" – number of likes you got for your posts
New followers	"New followers" – the number of follows and unfollows over time. This does not necessarily reflect your follower count.
Profile visits	"Profile visits" - number of profile views from your posts

Figure 10 presents the performance of the CHESS X social media. It is illustrated using metrics of Impressions (a), Engagement rate (b), Engagement (c), Post (d), Repost (e), Likes (f), New followers (g), and profile visits (h).

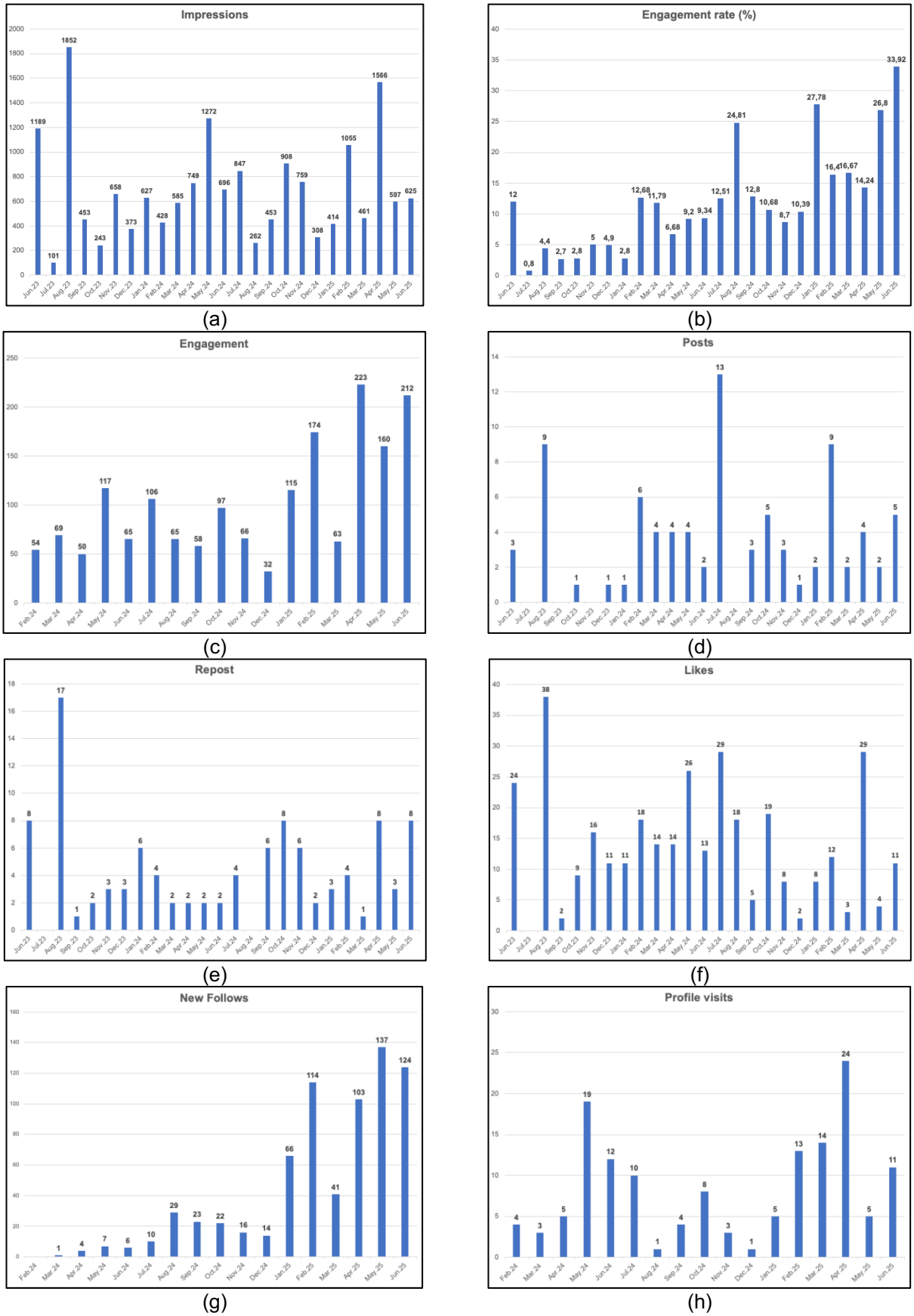


Figure 10: Performance of CHESS X Social Media Channel

On the 3rd of July, 2025, the CHESS X channel had 701 followers. Table 13 presents a one-year (04.07.2024-03.07.2025) summary of the CHESS X social media performance. The table presents the values extracted from the X analytic site.

Table 13: One-Year Summary of the CHESS X Social Media Performance

Metric	Value
Verified/total followers	701
Verified followers	39
Impressions	8133
Engagement rate (%)	16,7
Engagements	1366
Profile visits	98
Likes	146
Reposts	52
Bookmarks	2
Shares	3

5.3 Monitoring CHESS Facebook Social Media Channel

The Facebook social media channel is at https://www.facebook.com/ChessExcellenceHub. Its performance is measured using metrics listed in Table 14. This table also includes explanations of the metrics adapted from Facebook's Analytics site.

Table 14: Performance Metrics of the CHESS Facebook social media channel

Metric	Explanation
Reach	"Reach" counts reach from the organic or paid distribution of your Facebook content, including posts, stories and ads. It also includes reach from other sources, such as tags, check-ins and Page or profile visits.
Followers	"Followers" – the total number of followers of the Facebook Page/profile. This is calculated as the number of follows minus the number of unfollows over the lifetime of the page/profile.
Visits	"Visits" – a number of times the page/profile was visited.
Content interaction	"Content interaction" – a number of likes or reactions, saves, comments, shares and replies on the content. Content can include formats such as posts, stories, reels, videos and more.
Views	"Views" - a number of times your content was played or displayed.
Link clicks	"Link clicks" – a number of clicks, taps or swipes on links within the content, including ads. Content may include formats such as posts, stories, reels, and videos that lead to destinations or experiences.

Figure 11 presents the performance of the CHESS Facebook social media channel. It is illustrated using metrics of Reach (a), Followers (b), Visits (c), Content interaction (d), Views (e), and Link clicks (f).

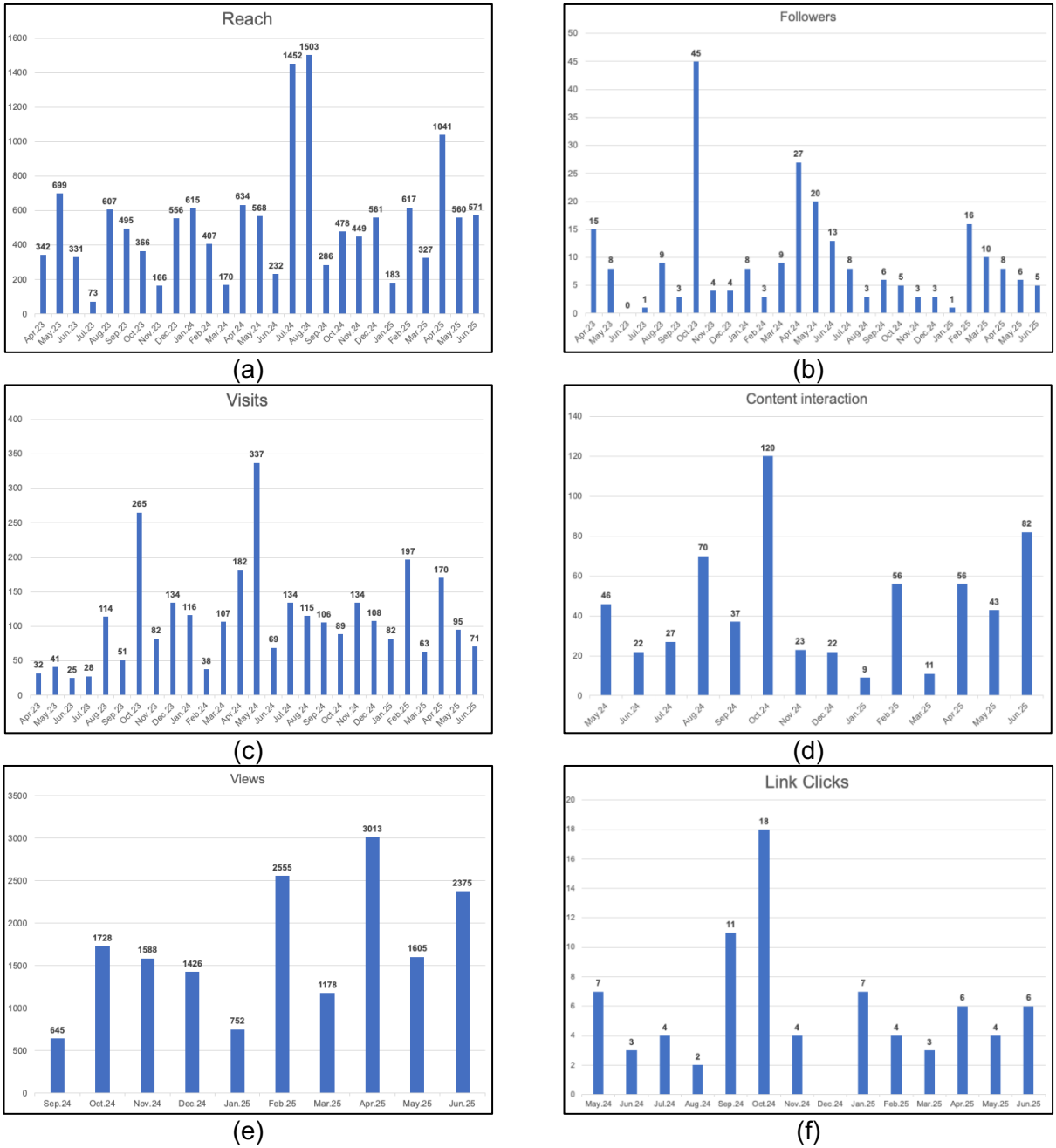


Figure 11: Performance of the CHESS Facebook Social Media Channel

Table 15 provides a monthly (i.e., average per month) summary of the CHESS Facebook channel performance.

Table 15: Summary of the CHESS Facebook Social Media Channel Performance

Metric	Average per month
Reach	529
Visits	111
Content interaction	45
Views	1687
Link clicks	5,6

On the 30th of June, 2025, the CHESS Facebook channel had 281 followers. Table 16 presents the three top cities and three top countries of the CHESS Facebook followers. In addition, Facebook provides the metrics of the followers' age and gender. This is aggregated demographic data, which is based on a number of factors, including age and gender information that users provide in their Facebook profiles. Table 17 presents these numbers taken on July 31, 2025.

Table 16: Top-Three Cities and Countries of the CHESS Facebook Followers

	Cities		Countries	
1	Tallinn, Harju County, Estonia	25,2%	Estonia	49,7%
2	Tartu, Tartu County, Estonia	19,6%	Lithuania	14%
3	Brno, Czech Republic	7,3%	Czech Republic	11,9%

Table 17: Age and Gender of the CHESS Facebook Followers

Age	Women	Men
18-24	1,8%	1,8%
25-34	9,1%	18,1%
35-44	10,9%	22,1%
45-54	11,2%	14,5%
55-64	2,2%	5,8%
65+	1,1%	1,4%
Total	**36,3%**	**63,7%**

5.4 Monitoring CHESS LinkedIn Social Media Channel

The Facebook social media channel is at https://www.linkedin.com/company/chess-cyber-security-excellence-hub/. Its performance is measured using metrics listed in Table 18. This table also includes explanations of the metrics adapted from the LinkedIn Analytics site.

Table 18: Performance Metrics of CHESS LinkedIn Social Media Channel

Metric	Explanation
Page views	"Page views" – represent the total number of times your company page has been viewed over a specific period.
New Followers	"New followers" – the change in your follower count over time, indicating how your audience is growing and whether your content is resonating.
Unique visitors	"Unique visitors" – the distinct number of individuals who have visited a specific page, post, or the overall platform within a given time frame.
Reactions	"Reactions" - emotional responses to your content. Users can select emojis to show that they like, celebrate, support, love, find insight, or feel curious about the content you share.
Members reached	"Members reached" – the number of unique users who have seen your content, such as a post or update
Impressions	"Impressions" – the number of times your content was displayed on LinkedIn, regardless of whether it was clicked or engaged with.
Engagement rate	"Engagement rate" – the percentage of people who interacted with your content (liked, commented, shared, clicked) compared to the number of impressions.
Clicks	"Clicks" – counted when a signed-in member clicks on the post, company name, or logo.

Figure 12 presents the performance of the CHESS LinkedIn social media channel. It is illustrated using metrics of Page views (a), New Followers (b), Unique visitors (c), Reactions (d), Members reached (e), Impressions (f), Engagement rate (g), and Clicks (h).

On the 30th of June, 2025, the CHESS LinkedIn social media had 1831 followers. Table 19 presents a monthly (i.e., average per month) summary of the LinkedIn channel performance. The estimated values are taken on the 30th of June, 2025.

In addition, two metrics are used – Visitor demographics and Follower demographics. Visitor demographics metrics, as defined in the LinkedIn Analytics site, are aggregated demographics of LinkedIn members when they visit the CHESS LinkedIn page. Follower demographics metrics are aggregated demographics of LinkedIn members who follow the CHESS LinkedIn page. Table 20 presents the top-three results regarding the job function, company size, industry, location and seniority both for the visitor and follower demographics. The period is one year, and the measurement is taken on July 31, 2025.

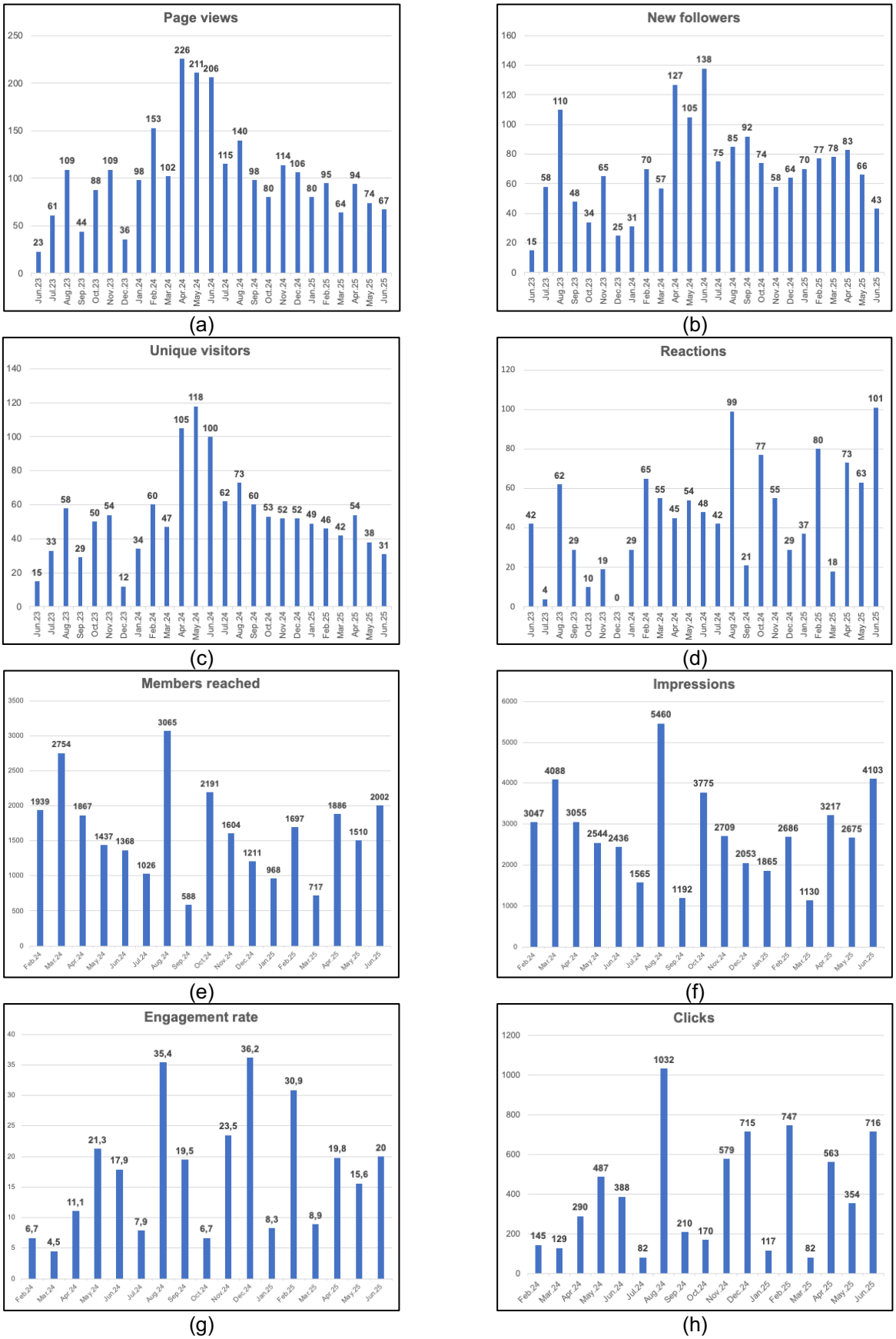


Figure 12: Performance of the CHESS LinkedIn Social Media Channel

Table 19: Summary of LinkedIn Channel Performance

Metric	Average per month
Page views	104,2
New followers	68,3
Unique visitors	52,4
Reactions	52,3
Members reached	1637,1
Impressions	2800
Engagement rate (%)	17,3
Clicks	400,4

Table 20: Top-Three Visitor and Follower Demographics Values

	Visitor demographics		Follower demographics	
Job function	Information technology	19,5%	Information technology	19,6%
	Education	14,4%	Education	16%
	Business development	7,8%	Engineering	10,2%
Company size	1001-5000 employees	21,2%	1001-5000 employees	21,6%
	51-200 employees	13,6	51-200 employees	13,5%
	201-500 employees	10,5%	11-50 employees	12%
Industry	IT services and IT consulting	20,7%	Higher education	24,1%
	Computer and network security	15,5%	IT services and IT consulting	13,6%
	Software development	12,1%	Software development	6,8%
Location	Tallinn metropolitan area, Estonia	11,7%	Tallinn metropolitan area, Estonia	12,5%
	Brno Metropolitan area, Czechia	10,8%	Tartu, Estonia	5%
	Greater Tartu area, Estonia	3,9%	Brno Metropolitan area, Czechia	4,9%
Seniority	Senior	35%	Senior	39,7%
	Entry	29,9%	Entry	27,9%
	Director	6,6%	Director	8,8%

5.5 Monitoring CHESS YouTube Channel

The YouTube channel is at https://www.youtube.com/channel/UCjuwIAQobUL7kQWBgb36y7Q. Its performance is measured using metrics listed in Table 21. This table also explains the metrics adapted from the YouTube Analytics site.

Table 21: Performance Metrics of CHESS YouTube Channel

Metric	Explanation
Views	"Views" – total views for the selected date range, region and other filters.
Watch time (hours)	"Watch time" – estimates total hours of viewing time of your content from your audience.
Average view duration	"Average view duration" – estimates average minutes watched per view for the selected content, date range, region and other filters.
Impressions	"Impressions" – estimates how many times the video thumbnails were shown to viewers.
Impressions clicks-through rate (%)	"Impressions clicks–through rate" – views per impressions shown. This measures how often viewers watched a video after seeing an impression.
Subscribers	"Subscribers" – the change in total subscribers found by subtracting subscribers lost from subscribers gained for the selected date range and region.

Figure 13 presents the performance of the CHESS YouTube channel. It is illustrated using metrics of Views (a), Watch time (hours) (b), Average view duration (c), Impressions (d), Impressions clicks-through rate (e), and Subscribers (f).

On the 30th of June, 2025, the CHESS YouTube channel had 18 followers. Table 22 presents a summary (both the average per month and total) of the YouTube channel performance.

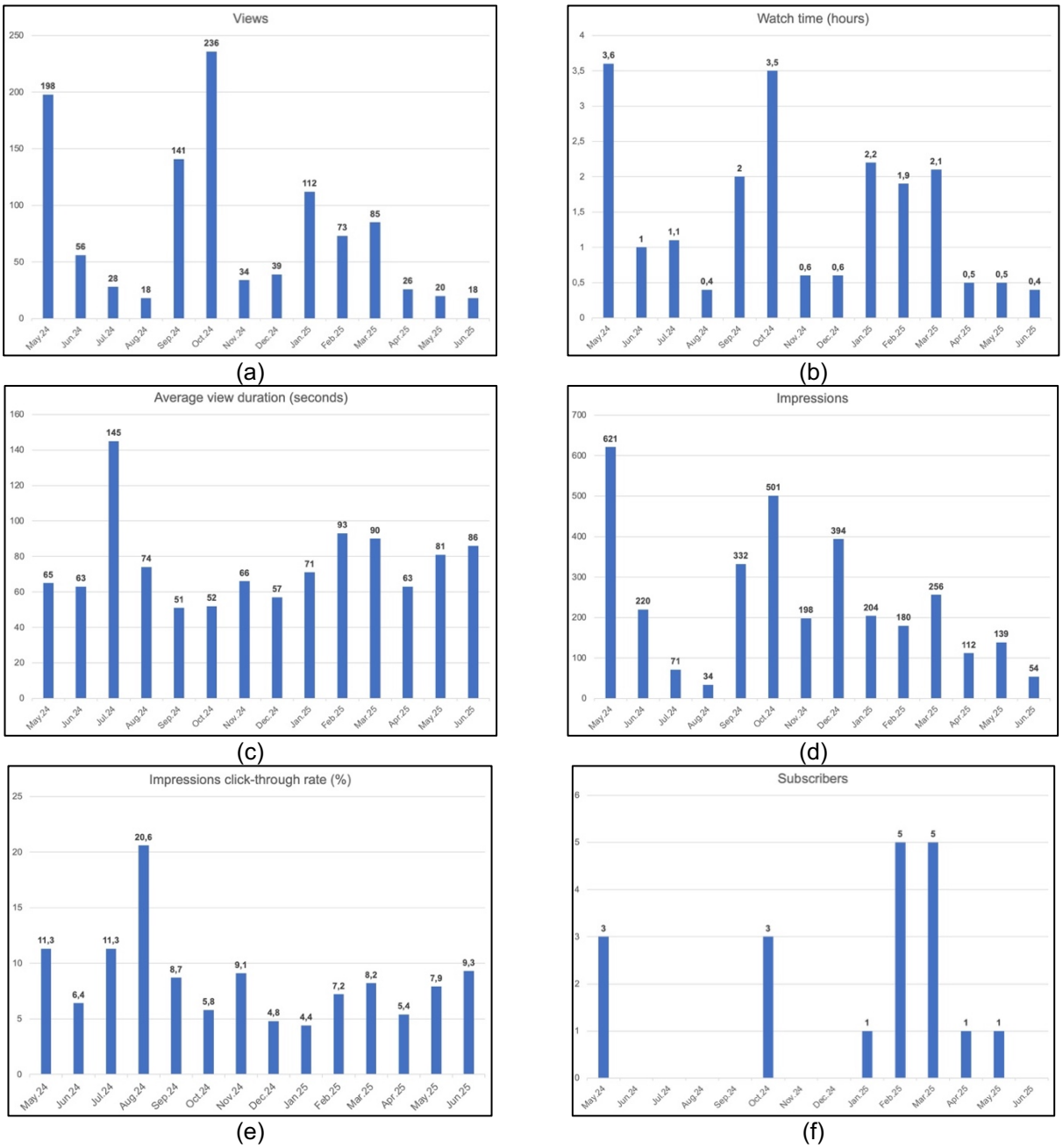


Figure 13: Performance of the CHESS YouTube Channel

Table 22: Summary of CHESS YouTube Channel Performance

Metrics	Average per month	Total
Views	77,4	1068
Watch time (hours)	1,5	26,3
Average view duration		1:28
Impressions	236,9	8057
Impressions clicks-through rate (%)		3,3%
Subscribers	1	18

5.6 Link Between the Objectives and KPIs

Table 23 illustrates the link between the CHESS key performance indicators and communication, dissemination, and exploitation objectives. The table provides the estimates for the M24 and M48 for 4 and 10 years after the project completion [1].

Table 23: 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 Dissemination and Exploitation Activities After CHESS

The CHESS project finishes on December 31, 2026. Once the project is over, several dissemination and exploitation activities will be continued. These activities will be strongly linked to the follow-up projects, such as:

- SecureNET (Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands), where four CHESS partners (UT, MUNI, Cybernetica, and RIA) will participate.
- CCAT (Cybersecurity Certification and Assessment Tools), where three CHESS partners (MUNI, Cybernetica and UTARTU) will participate.
- QARC (Quantum-Resistant Cryptography in Practice), where two CHESS partners

Dissemination: The CHESS website and the social media channels will remain active for at least 4 years. We plan to provide at least two newsletters regarding research results, training, awareness, and other security-related topics. These uptakes will be summarised from the CHESS follow-up projects, such as SecureNET, CCAT, and QARC[1] and promoted using the social media channels.

Similarly, the CHESS social media channels will be used to repost the results of the follow-up projects (SecureNET, CCAT, and QARC). CHESS will follow the social media channels of these projects and will repost significant uptakes in security research, training and awareness.

Exploitation: The CHESS project collects the project results regarding publications, presentations, theses, and videos. Deliverable D4.3 on *Materials from workshops and dissemination events* will be prepared at the end of the project by M48.

All the material will remain freely available at the CHESS Website and organised according to the research challenge areas. These results can be directly used in developing, creating, marketing or improving a product, process, or service, or shaping a policy that could positively impact the public's quality of life.

The CHESS results will be further exploited in the follow-up projects:

- SecureNET will echo CHESS, especially in the training and knowledge transfer needs [4]. CHESS recommends enhancing intersectoral collaboration and building stronger links between academic, business, and governmental partners to promote translating research findings into practice. Secondly, it recommends improving domain-specific education and training and understanding of technology transfer and IP issues. CHESS posits that it is essential to engage more in international cybersecurity initiatives. SECURE-NET will follow these recommendations to provide researchers with training opportunities and cross-sectoral experience and make partners more visible and active in the international cybersecurity arena.

[1] https://chess-eu.cs.ut.ee/2025/04/15/big-success-for-chess-new-cybersecurity-projects-funded/

- The CCAT project continues and builds upon the work carried out in the CHESS project, specifically in Challenge Area 2 (CA2) related to security certification. The CCAT tools will enable the assessment of TLS systems, evaluation of cryptographic devices and software libraries, including blackbox setups, testing of embedded security architectures (chips), and analysis of cybersecurity certification landscapes.
- The QARC project follows up on the Challenge Area 5 (CA5) focused on post-quantum cryptography. The main objective of QARC is to enhance the transition to quantum-safe cryptography through close collaboration among academia, businesses, and the public sector. QARC is focused not only on delivering and testing technical solutions resistant to quantum attacks but also on international networking, collaboration of national cybersecurity authorities, road mapping, and harmonisation across EU countries.

Table 23 presents several key performance indicators targeted to be achieved in the 4 years after the completion of the CHESS project. Ultimately, the CHESS partners will:

- Conduct research and publish co-authored scientific papers in high-impact journals
- Submit the research and innovation proposal
- Develop and deploy the security applications
- Supervise theses in security-related topics, potentially in collaboration with the industrial partners.
- Collaborate on the topics of security. This collaboration will potentially result in traineeship exchanges among the CHESS partners' institutions and between the regions.
- Conduct security-related training for researchers, industry, and NGOs.
- Organise security-related research, training, education, and awareness-raising events.

7 Concluding Remarks and Next Steps

This deliverable outlines the plan for communication, dissemination, and exploitation. It defines the objectives, identifies target audiences, and provides an overview of the strategic activities. The report then details the specific actions and tools for communication, dissemination, and exploitation, along with the monitoring approach. Finally, it highlights the planned dissemination and exploitation activities beyond the duration of the CHESS project.

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 the 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's existing websites to ensure accessibility. All partners will promote the project on their websites & social media.

We also start promoting the deployment and commercialisation 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 the 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 engage with expert audiences to raise awareness of the cross-regional strengths embodied in the CHESS project. CHESS plans to promote joint attendance at 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 organise dedicated dissemination workshops with potential user groups for deployment-ready results. Where appropriate, we will prepare newsletters and give interviews to promote our research. We will organise workshops, lectures and seminars engaging the public in cybersecurity R&I. Some will have an awareness-raising component, making the audience more perceptive of the risks they face in cyberspace. Others will be focused on popularisation, 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/

[3] CHESS: D4.2 Project Website, December 2023. Available https://chess-eu.cs.ut.ee/wp-content/uploads/2023/12/D4.2-Project-Website.pdf

[4] CHESS: D1.2 Strategy for Cross-Regional Collaboration in Cybersecurity, December 2024. Available https://chess-eu.cs.ut.ee/wp-content/uploads/2025/01/D1.2-Strategy-for-Cross-Regional-Collaboration-in-Cybersecurity.pdf

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 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, disseminating or communicating their activities or travelling within the project.

- Annex 3: Acknowledgement of EU funding.