Harmonizing People, Processes, and Technology for Robust Cybersecurity

D9.3 Mid-term report on dissemination, communication and clustering activities

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.cybersynchrony.eu/		
Deliverable	D9.3 Mid-term report on dissemination, communication and clustering activities		
Work Package	WP9 Dissemination, Exploitation and promotion		
Contractual due date	30/11/2024	**Actual submission date**	02/12/2025
Type	R (Report)	**Dissemination Level**	Public (PU)
Lead Beneficiary	eBOS Technologies Ltd (eBOS)		
Responsible Author	Eleni Keliri (eBOS)		
Contributions from	Violeta Vasileva (MAG), Kitty Kioskli (TRUST)		

Funded by the European Union

Funded by the European Union under Grant Agreement no. 101158555. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Issue Date	Changes	Contributor(s)
0.1	05.09.2025	ToC	Eleni Keliri (eBOS)
0.2	29.09.2025	First draft	Eleni Keliri (eBOS)
0.3	07.10.2025	Update Section 2, 3, and 4, 50% delivered for internal review	Eleni Keliri (eBOS), ALL
0.4	14.10.2025	Update content Section 5 and 6	Eleni Keliri (eBOS), Violeta Vasileva (MAG)
0.5	16.10.2025	Update content in all sections	Eleni Keliri (eBOS)
0.6	16.10.2025	98% ready for internal review and QA	Eleni Keliri (eBOS)
0.7	29.10.2025	Addressing comments from internal review, 95% delivered for peer-review and QA	Eleni Keliri (eBOS)
0.8	10.11.2025	Peer review	Kitty Kioskli (TRUST)
0.9	20.11.2025	Quality check	Sozos Karageorgiou (eBOS)
1.0	28.11.2025	100% final version ready for submission	Eleni Keliri (eBOS)

Disclaimer

The content of the document herein is the sole responsibility of the publishers, and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

Executive Summary 7
1 Introduction 8
1.1 Mapping CYberSynchrony Outputs 8
1.2 Linkage to other project outputs 9
1.3 Deliverable Structure 9
2 Dissemination & Communication (D&C) 10
2.1 D&C Plan & Strategy 10
2.2 CYberSynchrony Stakeholders 12
3 Dissemination Activities and Impact 13
3.1 Co-organization and/or participation in events 14
3.1.1 Training Programs 14
3.1.2 Webinars & Workshops 16
3.1.3 Exhibitions/Trade Fairs/ Symposiums 18
3.2 Scientific Publications 20
3.3 Bodies to disseminate project results 21
3.3.1 Bodies to push CYberSynchrony results 22
3.3.2 Standardization bodies/Open-Source initiatives 24
4 Communication Activities and Impact 26
4.1 Website 27
4.2 Social Media Accounts 28
4.2.1 LinkedIn 28
4.2.2 YouTube 31
4.2.3 X-Account 32
4.3 Newsletters & Emailing Lists 33
4.3.1 Subscription 33
4.4 Promotional Material 34
4.5 Multimedia 34
4.6 Public Talks 34
4.6.1 University Public Events 34
4.6.2 University Open Days 36
4.6.3 Events hosted by local entities and societal stakeholders 37
5 Impact (Analytics) 38
5.1 Google Analytics (Website) 38
5.2 LinkedIn 40
5.3 Mailchimp 41
6 Clustering Activities 43
6.1 Performed 43
6.2 Planned 45
7 Conclusions 46
8 References 47
Annex I – Multimedia: Initiation of the production of a promo animated video. 48
Annex II – D&C Tracker Tool 50

© CYberSynchorny, 2024

List of Figures

Figure 1. Outline of CYberSynchrony D&C Phases. Phases 1 & 2 are concluded. 10

Figure 2. Photos from the participation at CyberHOT 2025: Advancing Collaboration and Cybersecurity Training. 14

Figure 3. Capture of the Training Program, featuring CYberSynchrony presentation. 15

Figure 4. Dr. Eleni Seralidou (TRUST) presenting CYberSynchrony at the 20th TAROT Summer School. 15

Figure 5. Event Announcement banner. 15

Figure 6. Lectures during Cyber Security Winter School 2025. 16

Figure 7. Promotional banner of the Webinar: “From Risk to Resilience: Navigating the Cybersecurity Solutions Marketplace”. 16

Figure 8. SecRIot 2025 announcement banner. 18

Figure 9. Participation at the 8th NMIOTIC Conference. 18

Figure 10. eBOS participated in EU Cybersecurity Certification Day of the Digital Security Authority. 19

Figure 11. Presentation of Dr. Karvounidis featuring CYberSynchrony at the Cybersecurity Working Group of the ECGFF. 22

Figure 12. Prof. Nineta Polemi at the event/venue organised by the Special Interest Group A2 (Ports & Maritime) of the World Conference on Transport Research Society (WCTR). 23

Figure 13. FP delivering a presentation at CoDIT 2025. 23

Figure 14. CYberSynchrony represented by UPRC at CIE 2025, with roll-up banner and flyers. 24

Figure 15. MAG and IANUS presenting CYberSynchrony at ECSF Workshop in Brussels. 25

Figure 16. CYberSynchrony LinkedIn Page. 28

Figure 17. Examples of recent posts on LinkedIn and engagement. 29

Figure 18. An example of BYTE’s banner prepared and shared for the “Quotes on Cybersecurity” Campaign 30

Figure 19. An example of AMC’s banner prepared and shared for the “Meet Our Partners” Campaign 31

Figure 20. YouTube Channel content (video uploads & playlist). 32

Figure 21. CYberSynchrony’s X-Account 32

Figure 22. One-step Subscription through CYberSynchrony website: Newsletters - CYberSynchrony 33

Figure 23. Promotional material as displayed on the website. 34

Figure 24. Photos taken during the Workshop on Cybersecurity in Critical Sectors. 35

Figure 25. Photos taken during the Workshop on “Cybersecurity – Modern Trends and Concerns” 35

Figure 26. Roll-up banner and consortium partners showcasing CYberSynchrony at the CyberHOT 2025. 36

Figure 27. Focal Point representing CYberSynchrony at Career Days 2025 event with roll-up and flyers. 36

Figure 28. Dr. Elisavet Grigoriou presenting CYberSynchrony at the DEP InfoDay – Cyprus. 37

Figure 29. Google Analytics for the period October 2024 to November 2025, presenting the visitors of the website. 38

Figure 30. Google Analytics for the period October 2024 to November 2025, presenting the time spent on the website by visitors. 39

© CYberSynchorny, 2024

Figure 31. Engagement Analytics. 39
Figure 32. Map of visiting countries analytics. 40
Figure 33. LinkedIn analytics for Impression metrics (Nov 2024-Nov 2025) 40
Figure 34. Screenshot of Mailchimp contact list (blurred for GDPR). 42
Figure 35. List of campaigns (Newsletters) released and their performance analytics. 42
Figure 36. CYberSynchrony presentation during the official launch of the **CRACoWi Project** (Cyber Resilience Act – Compliance Wizard) at the kick-off. 44
Figure 37. Dr. Leandros Maglaras at the 1st CyberSuite workshop. 44

List of Tables

Table 1: Adherence to the GA 8
Table 2. CYberSynchrony D&C Phases and Goals achieved. 11
Table 3. CYberSynchrony Dissemination and Communication Target Groups and Interests. 12
Table 4. Dissemination channels and activities with KPIs achieved by M18. 13
Table 5. List of journal and/or conference publications & presentations by M18. 20
Table 6.Communication channels and activities with KPIs achieved by M18. 26
Table 7. LinkedIn posts for “Quotes on Cybersecurity” – Cybersecurity Awareness Campaign. 30
Table 8. LinkedIn posts for “Meet Our Partners” Campaign. 30

© CYberSynchorny, 2024

Acronyms and abbreviations

Abbreviation	Description
CA	Consortium Agreement
CMS	Content Management System
DCM	Dissemination and Communication Manager
DOA	Description of Action
EC	European Commission
GA	Grant Agreement
KPI	Key Performance Indicator
PCO	Project Coordinator
WP	Work Package
UC	Use Case(s)

© CYberSynchorny, 2024

Executive Summary

This deliverable D9.3 presents a comprehensive overview of the dissemination and communication (D&C) activities undertaken within the CYberSynchrony project, detailing strategies, stakeholder engagement, and the impact achieved across multiple channels up to M18. It aims to provide a clear understanding of how project outputs have been shared, promoted, and leveraged to maximize visibility, knowledge transfer, and engagement with relevant communities.

The document begins with an introduction outlining the mapping of CYberSynchrony outputs, their linkage to other project deliverables, and the structure of this deliverable itself. It then details the dissemination and communication plan and strategy, highlighting targeted stakeholders and the approaches used to ensure effective outreach.

A key focus of the deliverable is the description of dissemination activities, including co-organization and participation in events such as training programs, webinars, workshops, exhibitions, trade fairs, and symposiums. The report also reviews scientific publications generated by the project and identifies bodies and organizations that have actively contributed to promoting CYberSynchrony results, including standardization bodies and open-source initiatives.

The communication activities section addresses the various channels used to engage with the public and professional audiences, encompassing social media platforms (LinkedIn, YouTube, X), the project website, newsletters, online publishing, multimedia materials, promotional content, and public talks. Special attention is given to engagement with universities and societal stakeholders, as well as events aimed at broader community participation.

Finally, the deliverable presents an assessment of impact through analytics, including website metrics and social media performance, and summarizes clustering activities that facilitate collaboration and knowledge exchange with other projects and initiatives. Planned activities for continued dissemination and communication are also highlighted, ensuring sustainability and extended reach beyond the project lifetime.

Overall, D9.3 demonstrates the systematic approach taken by CYberSynchrony to disseminate knowledge, foster stakeholder engagement, and enhance the project's visibility, contributing to the long-term impact and societal relevance of its outputs.

© CYberSynchorny, 2024

1 Introduction

1.1 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony Grant Agreement (GA) commitments, as extracted from the formal deliverable and task description, with respect to their outputs and work to be performed.

Table 1: Adherence to the GA

Component no	Component title	Respective Chapter(s)	Justification
DELIVERABLE			
D9.3	Mid-term report on dissemination, communication and clustering activities	2- Dissemination and Communication Plan 3- Dissemination Activities 4- Communication Activities 5- Impact 6- Clustering Activities	The deliverable outlines the Dissemination and Communication plan & strategy, as well as the tools were employed, and the activities performed to achieve the project's KPIs. Specifically, in Chapter 2 the general D&C plan is presented including the strategy and the D&C Phases, while in Chapters 3 & 4 the Dissemination and Communication along with their KPIs are detailed, respectively. Chapter 4 includes also the social media accounts, and the website. Chapter 5 shows the impact through data and statistics of the D&C activities, while Chapter 6 outlines the effort on Clustering activities.
TASKS			
Task 9.1	Dissemination and Communication Activities	Chapters 2-5	In the present deliverable the Dissemination and Communication activities are detailed along with the specific tools and metrics of the D&C activities. Also, specific communication tools and activities are described as part of the communication strategy

© CYberSynchorny, 2024

		Chapter 6	of the project: newsletters, blog posts, social media accounts, website. Clustering activities with other projects under the thematic of cybersecurity and resilience.

1.2 Linkage to other project outputs

The deliverable guides and supports all other work across work packages, and it is the continuation of the previous deliverable D9.1.

1.3 Deliverable Structure

The document is structured as follows:

- **Section 2** describes the Dissemination and Communication Plan, including the D&C strategy, phases, and stakeholders
- **Section 3** introduces the Dissemination Tools and Activities, including the metrics (KPIs)
- **Section 4** introduces the Communication Tools and Activities, including the metric (KPIs)
- **Section 5** outlines the impact of the D&C activities
- **Section 6** presents the clustering activities performed and planned
- **Section 7** concludes the document.

© CYberSynchorny, 2024

2 Dissemination & Communication (D&C)

2.1 D&C Plan & Strategy

Figure 1 illustrates the various phases of the D&C strategy, with each phase aligned to a specific timeframe and targeting particular objectives to maximize the project's visibility and impact. Phases 1 and 2 have been completed, while Phase 3 was launched in Month 13.

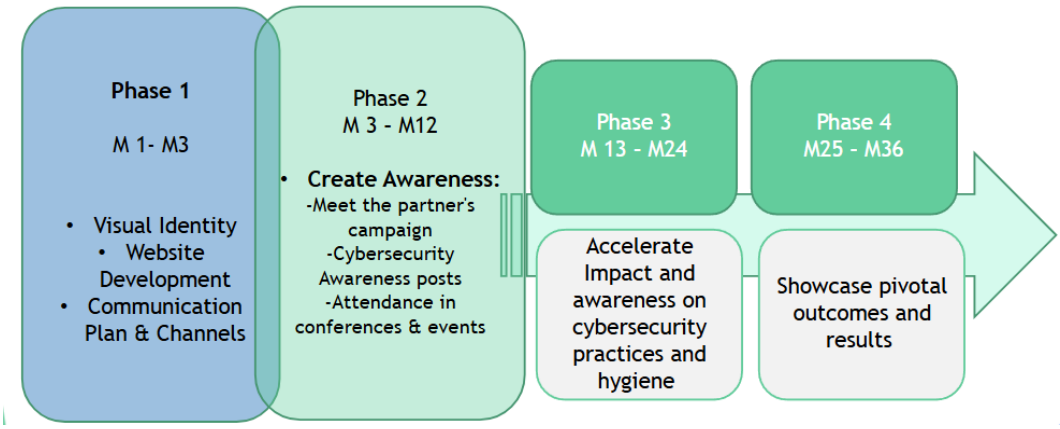

Figure 1. Outline of CYberSynchrony D&C Phases. Phases 1 & 2 are concluded.

- **Phase 1: M1 - M6 (Visual Identity, Website Development, Communication Plan & Channels) - *concluded***

The initial phase of the CYberSynchrony D&C strategy concentrated on establishing the foundation for the project's communication efforts. Key objectives during this stage included developing a cohesive visual identity, comprising the project logo, branding materials, and templates. The project website was also launched to function as the main platform for disseminating information, updates, and essential resources related to CYberSynchrony. In parallel, social media accounts were created to engage stakeholders and the wider audience, ensuring a consistent and strategic communication approach. This phase was successfully concluded with the submission of the previous Deliverable D9.1. However, all communication channels, including social media and the website, are regularly updated to maintain stakeholder engagement.

- **Phase 2: M6 - M12 (Create Awareness) - *concluded***

This phase, concluded in Month 12, focused on raising awareness of the project's goals and activities. During this phase, communication efforts became more active and outward facing, leveraging the channels and tools established in Phase 1. The objective was to ensure that relevant stakeholders, from industry professionals to the public, were informed about the project and its potential impact. Through targeted communication campaigns (e.g., "Meet our partners campaign"), social media engagement, and content sharing, CYberSynchrony successfully built a stronger presence and established initial connections with key audiences.

- **Phase 3: M13 - M24 (Accelerate Impact and Awareness on Cybersecurity Practices and Hygiene) - ongoing**

Phase 3 builds upon the awareness established in the previous phase, with a focus on accelerating the project's impact. This stage aims to deepen understanding and promote best practices in cybersecurity hygiene, while also launching campaigns related to CYberSynchrony's financial support to third parties (Month 16). The focus is on deepening understanding of cybersecurity hygiene and promoting actionable practices through targeted workshops, thematic discussions, and sector-specific events. To maximise reach between M13 and M24, dissemination will prioritise the most effective channels identified during earlier monitoring (e.g., LinkedIn), and EU cybersecurity networks. Communication efforts are contextualised within the broader European landscape

© CYberSynchorny, 2024

by referencing relevant initiatives and frameworks, including NIS2, the Cyber Resilience Act, ENISA guidance, and lessons emerging from other EU cybersecurity projects. Together, these measures aim to drive behavioural change, strengthen community adoption of robust cybersecurity practices, and demonstrate the project's tangible contribution to improving Europe's cybersecurity posture.

- **Phase 4: M25 - M36 (Showcase Pivotal Outcomes and Results) - *planned***

The final phase of the D&C strategy focuses on highlighting the key outcomes and results achieved throughout the project. By this stage, CYberSynchrony will have substantial accomplishments to communicate to stakeholders and the public. Communication efforts will concentrate on sharing these results through publications, reports, presentations, and multimedia content. This phase also aims to ensure the project's impact endures, maintaining visibility and engagement beyond its official completion. The website and other communication channels will continue to serve as lasting resources for showcasing the project's final achievements.

Each phase is tailored to the specific goals of CYberSynchrony, as presented in **Error! Reference source not found.**, ensuring a strategic and evolving communication plan that aligns with the project's progression.

Table 2. CYberSynchrony D&C Phases and Goals achieved.

Type of Information	Target Audience[1]	Channels	Goals	Achieved (justification)
D&C Phase 1 (M1-M06)				
Presentation of CYberSynchrony objectives and expected outcomes	A-F	Website Social Media Channels	Establish a project identity Gain general visibility Attracting potential collaborators and stakeholders	The website, social media accounts of the project were published, and the project identity was established through several material. The project gained general visibility through its social media accounts and engaged with potential stakeholders.
D&C Phase 2 (M06-M12)				
Presentation of elaborated Use Cases of CYberSynchrony & Create Awareness	A-C; E-F	Conferences, Workshops Promotional Material (Fact Sheets, Poster, Flyers) Newsletter Website Social Media Channels	Attracting potential collaborators and stakeholders	Partners attended and participated in several conferences. Promotional material such as Rollup banner, poster, leaflet, and fact sheet was prepared. 2 Newsletters were released and many posts on social media and website were created to raise awareness.

[1] Numbering as indicated in Table 3.

© CYberSynchorny, 2024

2.2 CYberSynchrony Stakeholders

The target groups, along with their corresponding interest for the project, are outlined in **Error! Reference source not found.** "CYberSynchrony Dissemination and Communication Target Groups and Interests".

Table 3. CYberSynchrony Dissemination and Communication Target Groups and Interests.

	Target Group	Interest for CYberSynchrony
A	Public Administration	Enhancing the security of e-governance platforms, safeguarding public trust, achieving national security goals, and ensuring compliance with data protection regulations.
B	Healthcare Institutions	Protecting sensitive patient data complying with healthcare specific cybersecurity regulations and ensuring uninterrupted service delivery.
C	Industries and SMEs	Fortifying organizational cybersecurity infrastructure, safeguarding proprietary and customer data, and ensuring operational continuity.
D	Research and Educational Institutions	Protecting intellectual property, ensuring the security of online educational platforms, and fostering a culture of cybersecurity awareness among students and staff.
E	Cybersecurity Service Providers and Consultants	Collaborating on advanced cybersecurity solutions, extending service offerings, and staying updated on the latest cybersecurity technologies and methodologies.
F	Public and Citizens	Benefiting from more secure digital services, safeguarding personal data, and enhancing awareness about potential cyber threats.
G	Regulatory and Compliance Bodies	Ensuring industries and sectors to adhere to cybersecurity regulations and fostering a more secure digital environment for all stakeholders.

© CYberSynchorny, 2024

3 Dissemination Activities and Impact

The dissemination strategy for the CYberSynchrony project was designed to maximize outreach and impact and outlined in Deliverable D9.1. It encompasses a wide range of activities aimed at engaging diverse stakeholders, including academic researchers, industry professionals, and the public. Core dissemination activities include publishing research findings in leading academic journals and presenting papers at international conferences to connect with the global research community. Additionally, the project produces technical publications and post to detail specific technologies and methodologies, while public deliverables ensure transparency and accessibility of key outcomes. Collectively, these efforts foster broad engagement and encourage knowledge sharing across multiple audiences.

By month 18, CYberSynchrony had already exceeded several key performance indicators (KPIs), reflecting remarkable progress and a strong commitment to the project's objectives, as shown in Table 4. The project has demonstrated exceptional engagement with the scientific and research community through active participation in conferences and workshops, as well as publishing results in peer-reviewed journals and conference proceedings. Its involvement into webinars and collaborative efforts through clustering activities with other projects is remarkable and enhances its reach across multiple target audiences. Moreover, from the outset, CYberSynchrony has maintained a robust presence on social media, building a vibrant community of professionals and enthusiasts and amplifying its overall impact.

Table 4. Dissemination channels and activities with KPIs achieved by M18

Dissemination channels and activities	KPIs	Target	Achieved by M18
Co-organisation and/or participation to events	Use case-based workshops	**3**	0
	Training Program	**1**	3
	Showcases	**>2**	0
	Webinars & Workshops	**>6**	5
	Exhibitions/Trade fairs/symposiums	**>3**	4
Scientific presentations	Scientific papers	**>6**	10
	Presentations in Scientific Conferences	**>6**	8
Bodies to Disseminate Project Results	Push CYberSynchrony results	**>2**	4
Standardization Bodies / Open-Source Initiatives	Push CYberSynchrony results	**>1**	2

© CYberSynchorny, 2024

3.1 Co-organization and/or participation in events

3.1.1 Training Programs

- **Participation at CyberHOT 2025: Advancing Collaboration and Cybersecurity Training in Crete**

The CYberSynchrony project was represented at the CyberHOT 2025 Summer School, held in Chania, Crete, under the auspices of the Technical University of Crete. The event gathered cybersecurity professionals, researchers, and representatives of EU-funded projects for an intensive, hands-on exploration of emerging challenges and innovations in the cybersecurity domain.

Figure 2. Photos from the participation at CyberHOT 2025: Advancing Collaboration and Cybersecurity Training.

On 27 May 2025, Dr. Violeta Vasileva (MAG), together with Xenia Economidou and Evangelos Michos (IANUS), presented CYberSynchrony during a dedicated R&D clustering session. On 30 May 2025, Dr. Vasileva delivered a specialized training session titled “A Practical Course on Social Engineering” as part of the summer school curriculum. The session examined the increasing sophistication of social engineering attacks, including AI-supported phishing and deepfake manipulation, through real-world case studies and hands-on exercises. More than 20 participants engaged in interactive discussions focused on practical tools for identifying and mitigating social engineering threats, particularly within critical infrastructure contexts. CYberSynchrony’s active participation in both the R&D and training tracks of the event underscores its commitment to promoting innovation, collaboration, and practical knowledge-sharing in support of a more resilient European cybersecurity landscape.

- **Presenting CYberSynchrony at the 20th TAROT Summer School**

From 30 June to 4 July 2025, the CYberSynchrony project participated in the 20th TAROT Summer School on Software Testing, Verification & Validation, held in Naples, Italy. The event brought together an international community of researchers, students, and industry professionals to explore the latest developments in software quality, testing, and security.

Representing CYberSynchrony, Dr. Eleni Seralidou and Dr. Kitty Kioskli (Trustilio B.V.) delivered a presentation outlining the project’s objectives, scope, and key activities. The presentation highlighted CYberSynchrony’s role in developing advanced cybersecurity skills and capabilities, fostering innovation, and enhancing resilience across European digital infrastructures. It also emphasized the project’s efforts to bridge the gap between academic research and industry needs in cybersecurity training and professional development. The TAROT network (Training And Research On Testing) provides a platform for knowledge exchange, mobility, and collaboration among students, faculty, and researchers in software and systems testing. The 2025 edition focused on testing and security, offering lectures, tutorials, and interactive sessions led by top experts from academia and industry. CYberSynchrony’s participation allowed early-stage researchers and PhD candidates to connect with the broader professional community, present their work, and gain insights into real-world cybersecurity challenges.

© CYberSynchorny, 2024

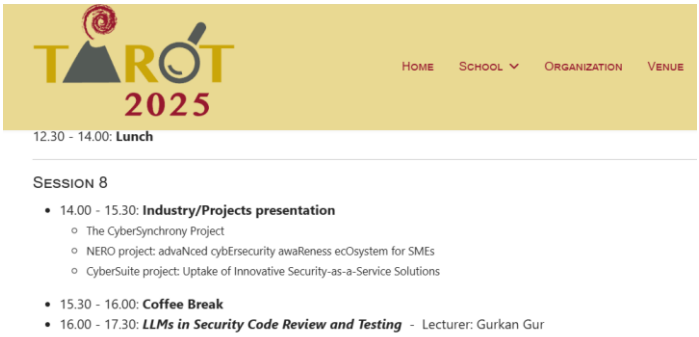

Figure 3. Capture of the Training Program, featuring CYberSynchrony presentation.

Figure 4. Dr. Eleni Seralidou (TRUST) presenting CYberSynchrony at the 20th TAROT Summer School.

- **Delivering training at the Cyber Security Winter School 2025**

Figure 5. Event Announcement banner.

CYberSynchrony took part in the Cyber Security Winter School 2025 in Lisbon, from 20 to 25 January. Partners from Trustilio, the University of Piraeus Research Centre (UPRC), Focal Point, and Maggioli S.p.A. contributed through technical sessions and collaborative discussions on critical topics, including the risks of vulnerable binaries and the configuration of intrusion detection systems. This participation reinforced CYberSynchrony's commitment to advancing cybersecurity skills, promoting innovation, and clustering with other EU-funded projects such as CyberSecPro to accelerate progress in cybersecurity education and practice.

Specifically, Dimitris Koutras (UPRC) delivered a session on "Navigating Cyber Threats: The Risk of Vulnerable Binaries", exploring the risks associated with vulnerable software and binaries in critical systems. Christos Lazaridis (FP) delivered a session on "Configuring and exploring **Suricata** logs through PFsense", showcasing a proper deployment and configuration of IDS solutions to the attendees, while MAG and TRUST actively contributed to the overall discussions. Our team's presence highlighted the project's commitment to contributing to a safer digital world while fostering strong connections with the broader cybersecurity community.

© CYberSynchorny, 2024

Figure 6. Lectures during Cyber Security Winter School 2025.

3.1.2 Webinars & Workshops

- **Joint webinar with the NERO, CyberSuite, and CyberSecPro projects "From Risk to Resilience: Navigating the Cybersecurity Solutions Marketplace"**

On January 29, 2025, CYberSynchrony proudly participated in the "Risk & Resilience: Navigating Cybersecurity Solutions Marketplace" webinar, organized by the NERO project. This insightful event brought together experts, researchers, and industry professionals to explore key challenges in cybersecurity risk management, resilience strategies, and emerging solutions in the cybersecurity marketplace.

The webinar featured contributions from multiple European cybersecurity projects, fostering discussions on best practices, innovative approaches, and collaboration opportunities within the ecosystem. It provided a valuable platform for sharing knowledge and strengthening synergies between research initiatives dedicated to enhancing cybersecurity resilience. Representing CYberSynchrony, Dr. Violeta Vasileva from Gruppo Maggioli (project coordinator) delivered a dedicated session. Her presentation provided an overview of the CYberSynchrony project, highlighting its objectives, expected impacts, and the three use cases (UCs) that drive its research and implementation. Her insights offered attendees a deeper understanding of how CYberSynchrony contributes to the advancement of cybersecurity solutions, ensuring robust and resilient security frameworks for organizations and infrastructures. This participation also served as a clustering activity, strengthening connections with other cybersecurity initiatives, including NERO, CyberSuite, and CyberSecPro. Engaging with these projects fosters knowledge exchange, promotes collaboration, and enhances the collective impact of European cybersecurity research.

Figure 7. Promotional banner of the Webinar: "From Risk to Resilience: Navigating the Cybersecurity Solutions Marketplace".

© CYberSynchorny, 2024

- **Focal Point delivered a Microsoft Sentinel Workshop (online)**

As part of CYberSynchrony's commitment to implementing cybersecurity awareness campaigns and educational programs, Focal Point organized a comprehensive 2-day online webinar titled "From Attack to Detection in Microsoft Sentinel" on July 7-8, 2025. This free training event, targeting university students across Europe, directly supported the project's objective to foster a culture of cybersecurity awareness and best practices across all levels of society. The workshop provided hands-on experience with Microsoft Sentinel, a leading SIEM platform, guiding participants through the complete attack lifecycle from understanding attacker tactics on Day 1 to detecting and responding to threats using real tools and guided labs on Day 2. By equipping the next generation of cybersecurity professionals with practical skills in threat detection and incident response, this initiative contributed to CYberSynchrony's broader goal of strengthening risk monitoring services and early detection of cyber incidents through advanced cybersecurity analytics tools, while simultaneously addressing the project's emphasis on harmonizing people, processes, and technology for robust cybersecurity infrastructure.

- **CYberSynchrony Advancing Cybersecurity Through Organization of Strategic Workshops**

The CYberSynchrony project, represented by our partner TRUST, has recently taken an active role in several key cybersecurity workshops:

  - **3rd ECSCI Workshop on Critical Infrastructure Protection & Resilience (ECSCI 2025)**

April 29–30, 2025 — Bilbao, Spain

Hosted at Tecnalia, this European Cluster for Securing Critical Infrastructures (ECSCI) event convened experts, innovators, and policymakers to tackle the complex interdependencies of modern critical infrastructures, spanning energy, transport, healthcare, finance, and more. Highlights included keynotes from ENISA, JRC, ECSO, and the European Commission, discussions on AI for resilience, IoT security, secure data sharing, and automated threat response. TRUST engaged in clustering and knowledge-exchange activities with other EU projects to drive strategic collaboration.

  - **3rd International Workshop on Cybersecurity of Critical National Infrastructures (CCNI 2025)**

May 27–30, 2025 — Fort Worth, Texas, USA

Co-located with IEEE WOWMOM, this workshop addressed the escalating risks facing critical national infrastructures, emphasizing the need for interdisciplinary approaches—technical, policy, human, and behavioural elements. TRUST supported the event as a member of the organizing committee, showcasing the CYberSynchrony and engaging in valuable clustering with other EU projects such as NERO, CyberSecPro, and CUSTODES.

  - **6th International Workshop on Security & Reliability of IoT Systems (SecRIoT 2025)**

June 9–11, 2025 — Lucca, Tuscany, Italy

Part of DCOSS-IoT 2025, SecRIoT 2025 brought together researchers and practitioners focused on the secure design, deployment, and operation of IoT systems. TRUST played a vital role in organising the workshop, fostering CYberSynchrony clustering with projects like NERO, CyberSecPro, CROSSCON, and others.

© CYberSynchorny, 2024

Figure 8. SecRIot 2025 announcement banner.

3.1.3 Exhibitions/Trade Fairs/ Symposiums

- **Participation at the 8th NMIOTC Conference on Cybersecurity in the Maritime Domain 2024**

The 8th NMIOTC Conference on Cyber Security in the Maritime Domain took place on 18–19 September 2024 in Chania, Crete, Greece, at the premises of the NATO Maritime Interdiction Operational Training Centre (NMIOTC). The conference addressed current and emerging cyber threats in the maritime environment, fostering collaboration among researchers, practitioners, naval personnel, academia, shipping companies, standardisation bodies, government agencies, international organisations, and both public and private sector stakeholders. Discussions focused on the latest trends in maritime cybersecurity, offering insights and guidance on countering complex and evolving cyber challenges. The event provided a platform for participants to exchange knowledge, debate critical issues, and strengthen cooperative efforts to enhance cybersecurity and cyber defence operations within the maritime domain.

The CYberSynchrony consortium was represented by its partners Trustilio (Dr. Kitty Kioskly) and the University of Piraeus Research Centre (UPRC) (Prof. Ninenta Polemi and Dimitris Koutras), who actively contributed to the conference discussions.

Figure 9. Participation at the 8th NMIOTIC Conference.

- **CYberSynchrony attended the Cybersecurity Days 2024 (Online)**

From 2 to 4 October 2024, the European Economic and Social Committee (EESC) and the Committee of the Regions (CoR) hosted the European Cybersecurity Month (ECSM) in Brussels. The event brought together leading experts from EU institutions, regional governments, and civil society to address the challenges of an evolving cybersecurity landscape.

© CYberSynchorny, 2024

CYberSynchrony consortium partner eBOS participated in the sessions held on Day 2 and Day 3 of the event. Day 2 topic was “Cybersecurity at the Sub-National Level” where discussions centred on the implementation of the NIS2 Directive, focusing on challenges and opportunities for regional and local authorities. Participants highlighted the need for stronger collaboration across governance levels and with the private sector, as well as the importance of addressing the cybersecurity skills gap. The concept of strategic autonomy and digital resilience was also emphasised as key to building a secure digital environment. Day 3 was on “ Social Engineering and Artificial Intelligence” where sessions explored the emerging risks of AI-powered social engineering attacks and their impact on cybersecurity strategies. The importance of cultivating a robust cybersecurity culture through continuous training and awareness was underlined. Participants also discussed the need for ongoing skills development and for establishing flexible, future-proof regulatory frameworks that can adapt to technological change. The key takeaways were: (a) The new EU cybersecurity regulation provides a common baseline for institutions and member states. (b) Regular risk assessments remain essential to identifying vulnerabilities and guiding mitigation efforts. (c) Addressing emerging threats, including AI-driven attacks and quantum computing risks, will require innovative and coordinated responses. (d) Regional authorities play a crucial role by supporting local entities through training, technical assistance, and knowledge sharing, and (e) Combating AI-based social engineering demands a collaborative, multi-layered approach across sectors.

- **CYberSynchrony at the EU Cybersecurity Certification Day of the Digital Security Authority**

The Digital Security Authority (DSA), as the National Cybersecurity Certification Authority (NCCA), organised the «European Cybersecurity Certification Day» on the 16th of October 2024. The event that took place at the iCTAcademy in Nicosia, Cyprus, focused on the European cybersecurity certification framework, highlighting the roles of various bodies involved in the implementation and oversight of cybersecurity standards. Starting with a welcome speech by Mr. George Michaelides (Commissioner of Communications), the agenda covered topics such as the Cybersecurity Act, European certification schemes, and the role of organizations like ENISA, national authorities, and conformity assessment bodies. The program featured key figures like Mrs. Ingrid Lauringson from the European Commission, Mr. Andreas Mitrakas from ENISA, and other experts in the field. The event concluded with networking breaks and a Q&A session that has provided opportunities for deeper engagement among attendees.

Figure 10. eBOS participated in EU Cybersecurity Certification Day of the Digital Security Authority.

- **Participation in “Boosting SMEs Cybersecurity Resilience” Conference**

On 10 October 2025, the CYberSynchrony project participated in the “Boosting SMEs Cybersecurity Resilience: Championing Skills to Secure Growth amidst Emerging Challenges” conference, held at the ICT Academy of the Office of the Commissioner of Communications in Cyprus. The event brought together experts, policymakers, and business leaders to explore strategies for enhancing cybersecurity resilience in small and medium enterprises (SMEs) within an increasingly complex digital landscape.

© CYberSynchorny, 2024

During the conference, Dr. Eleni Keliri (eBOS), engaged directly with attendees to announce the CYberSynchrony's upcoming Financial Support Open Calls, initiatives designed to provide SMEs with funding, guidance, and tools to strengthen their cybersecurity readiness. The announcement included the project's commitment to support SMEs in adopting best practices and building a more secure digital environment. The engagement received strong interest from participants, reflecting the growing awareness and investment in cybersecurity among SMEs. The event featured a series of presentations and discussions emphasizing skills development, innovation, and strategic collaboration as key drivers of resilience. CYberSynchrony's involvement reinforced the project's dedication to fostering knowledge exchange, partnerships, and practical initiatives that strengthen the cybersecurity ecosystem.

3.2 Scientific Publications

The dissemination activities of the CYberSynchrony project have already surpassed initial expectations, achieving and exceeding the established KPIs with a total of 10 scientific publications by M18, including two journal articles and eight conference papers, and two presentations in conferences/WGs. These outputs demonstrate the project's strong contribution to advancing research and innovation in cybersecurity. The journal publications, featured in high-impact academic venues, provide in-depth insights into the project's findings, while the conference papers have enabled active knowledge exchange and collaboration within the international research community. These accomplishments highlight CYberSynchrony's significant impact on the evolving cybersecurity landscape. All journal and conference publications are available on the CYberSynchrony website under Resources/ Publications section, with key details summarised in Table 5, along with the presentations at Scientific conferences.

Table 5. List of journal and/or conference publications & presentations by M18.

Paper Title	Journal	Partner	Year
Optimizing AI System Security: An Ecosystem Recommendation to Socio-Technical Risk Management	Human Factors in Design, Engineering, and Computing. AHFE (2024) International Conference	TRUST	2024
A Practical Human-Centric Risk Management (HRM) Methodology	Electronics, Special Issue Security Challenges and Opportunities of Artificial Intelligence/Big Data Scenarios	TRUST	2025
A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain	International Journal of Information Security	TRUST	2025
End-to-End Encryption: Technological and Human Factor Perspectives	Augmented Cognition (HCII 2025)	TRUST	2025
Cybersecurity Certification for Professional Training: An Overview	IEEE Education Engineering (EDUCON)	TRUST, UPRC	2025
Implementing the European Cybersecurity Skills Framework (ECSF): A Case Study of EU Innovation Projects	Vol. 24 No. 1 (2025): Proceedings of the 24th European Conference on Cyber Warfare and Security	TRUST	2025
Proposal of Harmonising Cybersecurity Professional Education and Training (CPET) in the European Union (EU): Exploratory Study	Vol. 24 No. 1 (2025): Proceedings of the 24th European Conference on Cyber Warfare and Security	UPRC	2025

© CYberSynchorny, 2024

Human Factors and Strategic Approaches in Cybersecurity: Threats for Critical Infrastructures in NIS2 Domains	Human Factors in Cybersecurity, AHFE International	UPRC	2025
Optimizing AI System Security: An Ecosystem Recommendation to Socio-Technical	Human Factors in Cybersecurity, AHFE International	TRUST	2024
Entitled: AI-Based MITRE ATT&CK Detection System: A Feasibility Study	11th IEEE/IFAC Conference on Control, Decision, and Information Technologies (CoDIT 2025)	FP	2025
Presentation Title	**Conference/WG**	**Partner**	**Year**
Cybersecurity Professional Education in the Maritime Sector	ECGFF Cybersecurity Working Group, "Cyber Resilience in Maritime & Port Logistics", Rome, Italy	UPRC, TRUST	May 2025
Implementing the European Cybersecurity Skills Framework (ECSF) for Maritime Cybersecurity Certified Professionals Using a Human-Centric Approach	WCTR SIGA2 Conference, Antwerp, Belgium	TRUST	May 2025

3.3 Bodies to disseminate project results

During the reporting period, the CYberSynchrony project disseminated its results through engagement with key **European and national bodies** involved in shaping cybersecurity policy and implementation. A major dissemination milestone was participation in the European Coast Guard Functions Forum (ECGFF), where the project contributed to the **Cybersecurity Working Group**. Through this forum, CYberSynchrony presented its work on cybersecurity education and capacity building, reinforcing its alignment with EU strategies on protecting critical maritime infrastructure. At the national level, CYberSynchrony actively engaged with the **Digital Security Authority (DSA)** of Cyprus and the **Office of the Commissioner of Communications** during the Digital Europe Programme (DEP) InfoDay and the Boosting SMEs Cybersecurity Resilience Conference. These events served as high-level platforms to showcase the project's cross-border cybersecurity framework and its Financial Support to Third Parties (FSTP) mechanism, designed to strengthen SME resilience and compliance with EU regulations such as NIS2 and the Cyber Resilience Act. The collaboration with these Cypriot authorities enhanced the project's outreach to public institutions and the private sector across Member States.

Furthermore, CYberSynchrony extended the dissemination of its research results within the European research and academic community through participation in events such as the **WCTR SIGA2 Conference**, the **CoDIT 2025,** and the **CIE 2025**. These platforms allowed the project to engage directly with academics, researchers, and industry representatives, promoting innovation in cybersecurity education, ethical AI, and workforce development. Especially CIE2025, had a strong collaboration with the Greek Computer Society (GCS/ΕΠΥ) and held under the auspices of the Greek Ministry of Education Religious Affairs and Sports, giving the opportunity to CYberSynchrony to engage with local stakeholder and key players.

Looking ahead, CYberSynchrony plans to establish closer collaboration with the **European Union Agency for Cybersecurity (ENISA)** to further align its research outcomes with EU cybersecurity strategies and to contribute to Europe's long-term cyber resilience objectives. Through these efforts, CYberSynchrony has fully met its dissemination KPI by engaging with at least three major bodies at the European, national, and academic levels, ensuring broad impact and sustainability of its results.

© CYberSynchorny, 2024

3.3.1 Bodies to push CYberSynchrony results

- **CYberSynchrony represented at the ECGFF Cybersecurity Working Group**

From 6 to 8 May 2025, the CYberSynchrony project was represented by partners University of Piraeus Research Center (UPRC) and Trustilio (TRUST) at the Cybersecurity Working Group of the European Coast Guard Functions Forum (ECGFF), held in Rome under the joint Italian and French Chairmanships. The event, titled "Cyber Resilience in Maritime & Port Logistics", convened experts from across Europe to discuss pressing cybersecurity issues in the maritime domain, including AI and IoT security, risks in port logistics, regulatory challenges, and cybersecurity training. The discussions aimed to strengthen international cooperation and develop a coordinated approach to securing maritime and port infrastructures.

During the event, Dr. Theodoros Karvounidis (UPRC) delivered a presentation on "Cybersecurity Professional Education in the Maritime Sector." His intervention underscored the ongoing digital transformation of maritime systems and the emerging cyber threats they face, emphasizing the need to upskill maritime professionals to safeguard critical infrastructure. He also highlighted the contribution of European initiatives such as CYberSynchrony, CyberSecPro, and NERO in promoting workforce development, as well as their alignment with the European Cybersecurity Skills Framework (ECSF) to harmonize training standards across Europe.

Dr. Karvounidis further presented CYberSynchrony's objectives in supporting threat monitoring, incident response, and cross-border cooperation through advanced training and virtual cyber range platforms. Participation in this event strengthened CYberSynchrony's engagement within the European maritime cybersecurity community and reinforced the project's commitment to international collaboration, skills development, and public-private partnerships in advancing maritime cyber resilience.

Figure 11. Presentation of Dr. Karvounidis featuring CYberSynchrony at the Cybersecurity Working Group of the ECGFF.

- **Presentation at the WCTR SIGA2 Conference 2025**

From 7 to 9 May 2025, the CYberSynchrony project participated in the WCTR SIGA2 Conference, held in Antwerp, Belgium. The three-day international event was organised by the Special Interest Group A2 (Ports & Maritime) of the World Conference on Transport Research Society (WCTR) in collaboration with the University of Antwerp. The conference served as a dynamic forum for advancing scientific and policy-oriented discussions relevant to the transport and maritime sectors.

CYberSynchrony was represented by project partner Trustilio (TRUST), who delivered a presentation entitled "Implementing the European Cybersecurity Skills Framework (ECSF) for Maritime Cybersecurity Certified Professionals Using a Human-Centric Approach." The presentation outlined how the ECSF can be applied within the maritime sector to enhance professional certification, strengthen workforce capabilities, and promote a unified skills framework across Europe. The SIGA2 Conference is designed to foster interdisciplinary dialogue by integrating academic research, industry expertise, and policy insights.

© CYberSynchorny, 2024

Its unique format encourages open idea development without the requirement of formal papers and features interactive sessions, port visits, and cultural exchanges. CYberSynchrony's participation contributed to strengthening collaboration between research and practice, reinforcing its role in advancing maritime cybersecurity education and workforce development.

Figure 12. Prof. Nineta Polemi at the event/venue organised by the Special Interest Group A2 (Ports & Maritime) of the World Conference on Transport Research Society (WCTR).

- **Sharing our mission to drive ethical AI in cybersecurity at CoDIT2025 in Split, Croatia**

From 15 to 18 July 2025, the CYberSynchrony project was represented by Focal Point sprl at the 11th IEEE/IFAC Conference on Control, Decision, and Information Technologies (CoDIT 2025) in Split, Croatia. The conference provided a prominent forum for over 800 submissions, 79 technical sessions, four keynote talks, and a dedicated Women-in-Engineering program, bringing together experts from academia, industry, and research organizations.

During the event, the CYberSynchrony team presented on the role of ethical AI in cybersecurity, highlighting how AI can enhance blue-team operations by providing real-time threat detection, transparent algorithms, and analyst-guided defence strategies. The presentation emphasized the importance of integrating ethical principles into AI systems to ensure that cyber defence solutions not only respond to threats but also prioritize privacy, accountability, and anticipatory protection measures. CYberSynchrony's participation in CoDIT 2025 reinforced the project's commitment to advancing responsible AI applications in cybersecurity, fostering innovation while promoting ethical standards in the development and deployment of next-generation threat detection and mitigation systems.

Figure 13. FP delivering a presentation at CoDIT 2025.

© CYberSynchorny, 2024

- **Participating in CIE 2025 Conference on Informatics in Education, Piraeus, Greece**

The 17th Conference on Informatics in Education (CIE2025) was organized by the Department of Informatics of the University of Piraeus, the Department of Informatics of the Ionian University, and in collaboration with the Greek Computer Society (GCS/ΕΠΥ). The 17th CIE2025 was held under the auspices of the Greek Ministry of Education Religious Affairs and Sports. The conference occurred as a Digital-conference (online) on November 7 and 8, and as synchronous meeting at Piraeus University with online attendance on 9 November 2025. During the physical part of the meeting a roll-up banner showcased to the participants while >150 flyers were distributed by our project partners from UPRC.

Figure 14. CYberSynchrony represented by UPRC at CIE 2025, with roll-up banner and flyers.

3.3.2 Standardization bodies/Open-Source initiatives

- **European Cybersecurity Skills Framework (ECSF) Workshop 2025**

On the 20-21st of November 2025, the "Engaging EU Projects Using the European Cybersecurity Skills Framework (ECSF)" Workshop, organised by ENISA, gathered a wide range of experts, policymakers, educators, and representatives from EU-funded cybersecurity initiatives to exchange insights on the application of the ECSF in advancing cybersecurity skills development. The event served as an important platform for collaboration, focusing on harmonizing training efforts, aligning educational outcomes with industry needs, and promoting a unified approach to skills recognition across Europe. For instance, the workshop brought together representatives from a diverse range of EU-funded cybersecurity initiatives, including AKADIMOS, Cadmus, CURIUM, CyberActioning, CyberFort, CyberGuard, CyberHubs, CyberMACS (Erasmus Mundus), CyberSec4OT, CyberSecPro, CYberSynchrony, CYBERUS (Erasmus Mundus), CYCERONE, Digital4Security, EU-Inspire, and NERO, fostering collaboration and knowledge exchange across these complementary projects.

The CyberSynchrony project was represented by Dr. Violeta Vasileva (MAG) and Demetris Antoniou (IANUS), who delivered a presentation titled "CyberSynchrony and ECSF". Their session highlighted how the project integrates the ECSF into its activities to support consistent skill mapping, strengthen workforce readiness, and foster synergy with other European cybersecurity initiatives.

The workshop's discussions emphasized the value of using the ECSF as a shared framework for bridging the gap between education, research, and professional practice. Participants collectively recognized the need for closer cooperation between EU projects to ensure alignment in developing and assessing cybersecurity competences. Key takeaways included the establishment of shared repositories of ECSF-aligned materials, the promotion of joint events and knowledge exchange mechanisms, and the reinforcement of partnerships between academia, industry, and public bodies. CYberSynchrony's active involvement in the workshop underscored its commitment to advancing a coordinated European approach to cybersecurity capacity building.

© CYberSynchorny, 2024

Moving forward, continued engagement with ECSF-related initiatives will further enhance the project's impact in promoting digital resilience, skills development, and professional mobility across the European cybersecurity ecosystem.

Figure 15. MAG and IANUS presenting CYberSynchrony at ECSF Workshop in Brussels.

- **Open-Source initiative: Gitlab**

As part of our open-source initiatives, we leverage open-source tools such as GitLab and Docker to support the development and deployment of CYberSynchrony modular framework. These tools enable automated workflows for building, testing, and deploying software, ensuring consistency and efficiency across our processes. GitLab serves as our central platform for version control, continuous integration, and continuous deployment (CI/CD). Using GitLab pipelines, we automate the building, testing, and pushing of Docker images to our registries, ensuring that each iteration of CYberSynchrony is consistent, reproducible, and ready for deployment.

By relying on open-source tools, we not only reduce dependency on proprietary software but also foster a culture of transparency and collaboration. Our workflows can be shared and adapted by the broader community, and the use of standard open-source technologies ensures interoperability and scalability. Additionally, this approach allows our teams to quickly iterate, detect issues early through automated testing, and maintain a seamless integration process across multiple environments, all while staying aligned with open-source principles, whenever we can.

© CYberSynchorny, 2024

4 Communication Activities and Impact

The communication strategy of CYberSynchrony is designed to maximize visibility and engagement across multiple stakeholder groups through a coordinated mix of traditional and digital outreach channels. Building on the foundation established in the previous period, the consortium continues to leverage its internal communication assets and partner networks to ensure consistent dissemination of key messages aligned with the project's objectives and scope.

High-quality promotional materials, including updated roll-up banners, flyers, and brochures developed by eBOS Technologies have been produced and distributed at major events, workshops, and conferences. These materials are instrumental in communicating the project's mission, technical innovation, and societal impact. Complementing these physical assets, the project maintains an active digital presence through its LinkedIn, X (Twitter), and YouTube channels, which are regularly updated with announcements, event highlights, and educational content focused on advancing cybersecurity awareness and resilience.

In addition, press releases, newsletters, and public engagement activities, including participation in open days, info sessions, and panel discussions have strengthened CYberSynchrony's visibility across both the research community and the broader public. These communication actions contribute to establishing the project as a recognizable and trusted initiative within the European cybersecurity landscape. Ongoing monitoring of communication KPIs ensures that outreach remains effective, inclusive, and aligned with project goals. A detailed overview of KPI performance and upcoming targets is provided in Table 6 of this report.

Table 6.Communication channels and activities with KPIs achieved by M18.

Communication channels and activities	KPIs	Target	Achieved by M18
Project Website	From M03 to Y06	**released**	Released by M03
Online Publishing	Press releases on website	**≥ 12**	25
	Articles to newspapers, magazines and online publishing platform Different platforms for posting	**≥ 10** **>4**	8 4
Social media	Social media followers by M36 **> 1000** Average monthly impressions **> 500**	**>1000** **>500**	212 2302
E-Newsletter	Twice a year starting from **M06** Issued Contact list	**>10** **>1000**	2 (+1) 245
Promotional Material	Number of distributed printed materials (e.g., brochures, flyers); Display banners	**>3000** **>3**	520 4
Multimedia	Produced videoclips Conducted interviews Videoclip views	**3** **>6** **>10,000**	0 10 (2 released) NA

© CYberSynchorny, 2024

Public Talks	University public events Attendees per event	**>3** **>60**	5 50-100
	University open days	**>3**	1
	Events hosted by local entities and societal stakeholders Public attendees per event	**>4** **>120**	3 150-200

4.1 Website

The CYberSynchrony project website serves as the primary digital hub for disseminating information about the project, its objectives, activities, and outcomes to a wide range of stakeholders. Designed for accessibility and ease of navigation, the website provides up-to-date content on project milestones, events, publications, news, and open calls, ensuring that both the cybersecurity community and the public can stay informed about the project's progress.

The website also hosts downloadable resources, including brochures, flyers, and technical materials, as well as links to the project's social media channels and YouTube content. This integration facilitates cross-platform engagement, encouraging visitors to explore multimedia content and follow CYberSynchrony's ongoing activities. Regular updates to the website ensure continuous visibility and transparency of the project's work. The platform also supports stakeholder engagement by providing contact information, making it a key tool for knowledge dissemination, networking, and promoting the project's impact across Europe and beyond.

The CYberSynchrony website is organized to provide intuitive navigation and easy access to relevant project information for diverse audiences. The main menu tabs include:

- **Home**: Serves as the landing page, providing a concise overview of the project, its mission, key objectives, and latest news highlights.
- **About**: Details of the project's scope, vision, expected impacts, consortium partners, and governance structure. This section introduces visitors to the overall framework and strategic priorities of CYberSynchrony.
- **Use Cases**: Presents the project's three primary use cases, outlining their objectives, technical approaches, and expected outcomes. This section demonstrates real-world applications of the project's research and innovations.
- **News & Events**: Shares updates on project activities, participation in conferences, workshops, webinars, and other dissemination initiatives. It keeps stakeholders informed about ongoing progress and opportunities for engagement
- **Resource**s: Provides downloadable materials such as brochures, flyers, technical reports, and guidelines, enabling stakeholders to access detailed information about the project.
- **Contact**: Offers contact details for inquiries, collaboration proposals, and general engagement with the project team, facilitating stakeholder interaction and networking.
- **NEW ADDITION** - ***Open Calls****: Highlights opportunities for SMEs and public bodies to participate in CYberSynchrony initiatives, including the Financial Support to Third Parties (FSTP) program, supporting wider engagement and project uptake. (not visible yet. To be released by M22)*

The website is regularly updated, with all the activities and resources available. Also, a full list of public deliverables is available under the Resources Tab here.

© CYberSynchorny, 2024

4.2 Social Media Accounts

4.2.1 LinkedIn

The CYberSynchrony LinkedIn account continues to serve as a central hub for professional engagement, connecting the project with a wide network of stakeholders across the cybersecurity, ICT, and policy domains. It provides regular updates on project milestones, event participation, research outputs, and cross-project collaborations, reinforcing CYberSynchrony's role as a thought leader in European cybersecurity innovation.

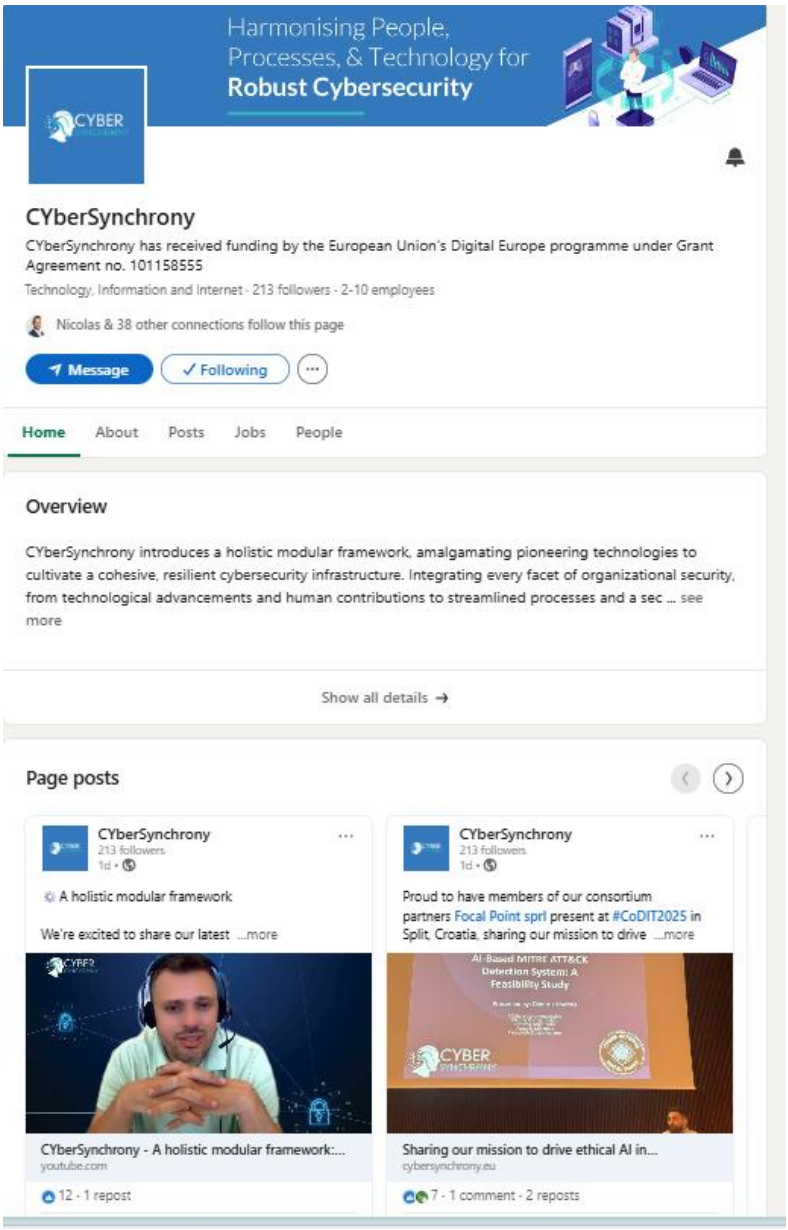

Figure 16. CYberSynchrony LinkedIn Page.

Through curated content and strategic communication campaigns, the LinkedIn platform fosters a growing community of professionals, researchers, and policymakers, promoting interaction and collaboration around shared challenges and emerging solutions. By showcasing success stories, sharing event coverage, and amplifying partner activities, the CYberSynchrony LinkedIn presence plays a key role in enhancing project visibility, supporting clustering activities, and building trust across the European digital ecosystem. Examples of posts are shown in Figure 17.

© CYberSynchorny, 2024

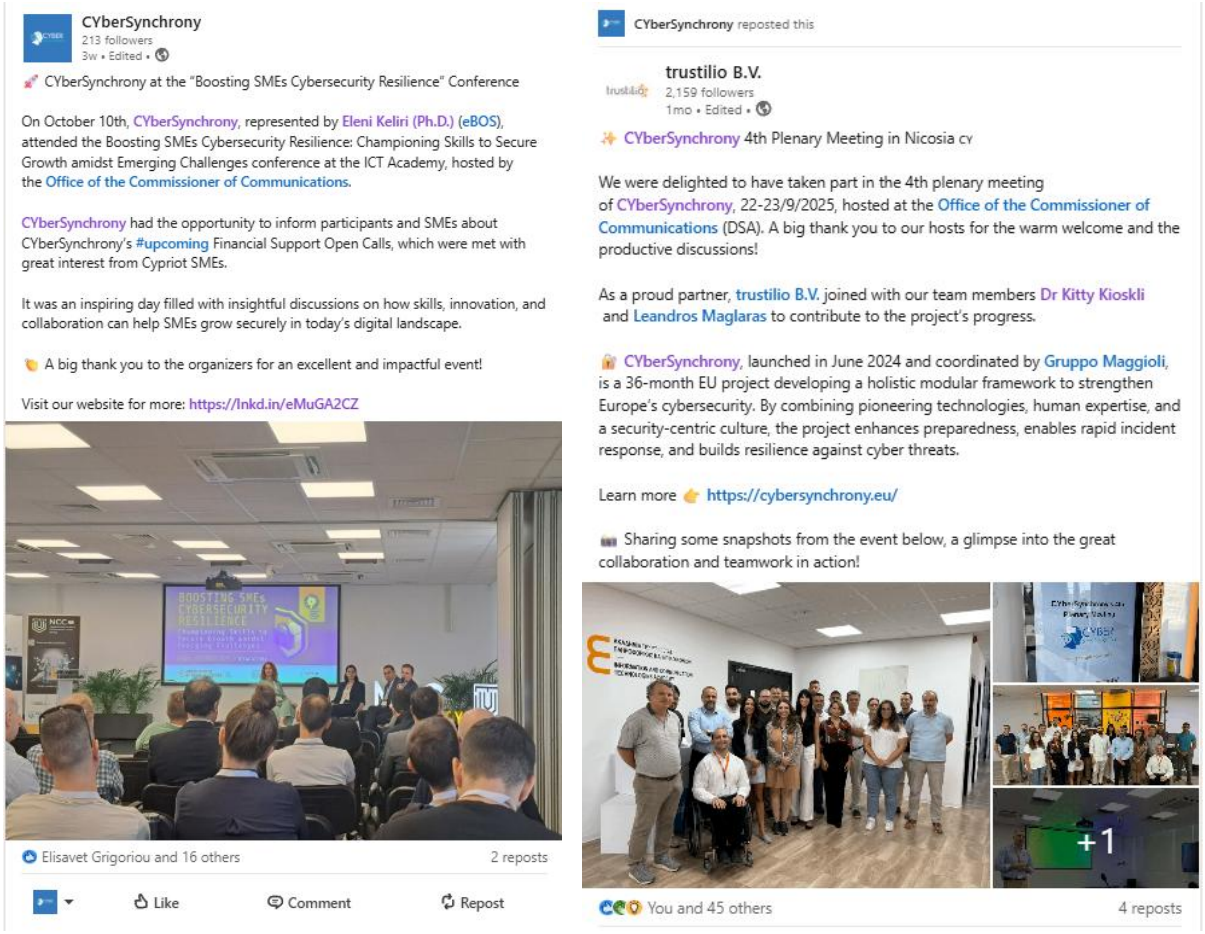

Figure 17. Examples of recent posts on LinkedIn and engagement.

- "Quotes on Cybersecurity" – Cybersecurity Awareness Campaign

To further enhance engagement and promote awareness around the project's mission, CYberSynchrony launched the "Quotes on Cybersecurity" cybersecurity awareness campaign on LinkedIn between December 2024 and May 2025, sharing 2 posts per month (Table 7). Example of the prepared material is presented in Figure 18. This initiative invited project partners to share short, thought-provoking quotes or reflections on key cybersecurity challenges, values, and opportunities shaping Europe's digital future. Each post featured a partner representative's personal insight, accompanied by the project's branding and visuals, creating a unified and relatable communication thread across the consortium. The campaign successfully humanized complex cybersecurity topics, fostering dialogue among professionals, researchers, and policymakers while strengthening the project's online presence. By combining expertise with creativity, the initiative contributed to building a strong, community-oriented identity for CYberSynchrony within the European cybersecurity landscape.

- "Meet Our Partners" Campaign

As part of its continuous D&C strategy, CYberSynchrony launched the "Meet Our Partners" campaign on LinkedIn between December 2024 and May 2025 (Table 8). The campaign is planned to continue for the remaining 7 partners and specifically run again from June to December 2026 with one post per month. The campaign aims to highlight the diverse expertise and contributions of the project's consortium members, showcasing their roles in advancing cybersecurity innovation, research, and capacity building within the European digital ecosystem. Each post introduced one partner organization, outlining its core competencies, project responsibilities, and unique contribution to CYberSynchrony's objectives. An example of the prepared material for one of our partners (AMC), is given in Figure 19. This initiative not only strengthened the project's online visibility but also promoted transparency, collaboration, and stakeholder engagement. The campaign achieved strong engagement metrics

across the project's social media channels, attracting new followers, expanding its professional network, and reinforcing CYberSynchrony's position as a collaborative and forward-looking EU-funded initiative.

Table 7. LinkedIn posts for "Quotes on Cybersecurity" – Cybersecurity Awareness Campaign.

Partner	Date	Link to post
TRUST	12/12/2024	https://www.linkedin.com/feed/update/urn:li:activity:7272590829418864640
IANUS	19/12/2024	https://www.linkedin.com/feed/update/urn:li:activity:7275458538573885442
AMC	09/01/2025	https://www.linkedin.com/feed/update/urn:li:activity:7283029749503864832
EBOS	23/01/2025	https://www.linkedin.com/feed/update/urn:li:activity:7288103197183758336
MAG	07/02/2025	https://www.linkedin.com/feed/update/urn:li:activity:7293584757672587264
DSA	21/02/2025	https://www.linkedin.com/feed/update/urn:li:activity:7298597341069004800
FP	07/03/2025	https://www.linkedin.com/feed/update/urn:li:activity:7303678302811025409
MER	21/03/2025	https://www.linkedin.com/feed/update/urn:li:activity:7308744240656764928
BYTE	04/04/2025	https://www.linkedin.com/feed/update/urn:li:activity:7313802548556017664
EGL	18/04/2025	https://www.linkedin.com/feed/update/urn:li:activity:7318876037759569921
UPRC	09/05/2025	https://www.linkedin.com/feed/update/urn:li:activity:7326486150280372224

Table 8. LinkedIn posts for "Meet Our Partners" Campaign.

Partner	Date	Link to post
MAG	15/01/2025	https://www.linkedin.com/feed/update/urn:li:activity:7285189038586691584
IANUS	14/02/2025	https://www.linkedin.com/feed/update/urn:li:activity:7296066344821673984
EBOS	14/03/2025	https://www.linkedin.com/feed/update/urn:li:activity:7306207507654299648
AMC	11/04/2025	https://www.linkedin.com/feed/update/urn:li:activity:7316339301166821376
UPRC	14/05/2025	https://www.linkedin.com/feed/update/urn:li:activity:7328298085833404416

Figure 18. An example of BYTE's banner prepared and shared for the "Quotes on Cybersecurity" Campaign

© CYberSynchorny, 2024

Figure 19. An example of AMC's banner prepared and shared for the "Meet Our Partners" Campaign

4.2.2 YouTube

The CYberSynchrony YouTube channel serves as a central platform for video sharing and knowledge dissemination within the cybersecurity community. It will host engaging content that communicates the project's objectives, research outputs, and innovative solutions. As part of this effort, the D&C Manager (eBOS) has planned and executed an interview series. The interview series aims to highlight each partner's role within the consortium, their specific expertise, and their perspective on how CYberSynchrony contributes to strengthening Europe's cybersecurity ecosystem. Each video features a short discussion on the partner's technical activities, innovative approaches, and expected impact on industry and research. These interviews not only provide an accessible way to communicate the project's progress but also humanize its collaborative nature, giving visibility to the individuals and organizations driving its success.

The videos will be gradually released through the YouTube channel and cross-promoted via the project's LinkedIn and X (Twitter) accounts to maximize outreach and audience engagement. This coordinated dissemination effort ensures consistent messaging across platforms, reinforcing the project's identity and expanding its digital footprint within the European cybersecurity community. The series will also serve as a long-term communication asset, offering reusable multimedia content for future presentations, clustering events, and stakeholder engagement activities. In total 10 interviews were conducted, and the posting has initiated in October 2025. The goal is to release 1 interview per month, so in a period of 10 months (June 2026) all the interviews to be publicly available.

To date, the channel has published two interviews with project partners, providing insights into the project's impact, technical achievements, and contributions to European cybersecurity (Figure 20). These interviews offer stakeholders a direct perspective from the consortium, reinforcing transparency and engagement. Looking ahead, CYberSynchrony plans to produce a high-quality animated promotional video, designed to visually summarize the project's objectives, use cases, and societal impact, further increasing engagement and outreach across diverse audiences. Through this dynamic platform, the YouTube channel enhances project visibility, encourages collaboration, and fosters discussion among researchers, professionals, and stakeholders. By sharing high-quality visual content, CYberSynchrony strengthens its role in promoting cybersecurity knowledge, skills development, and the adoption of innovative practices.

© CYberSynchorny, 2024

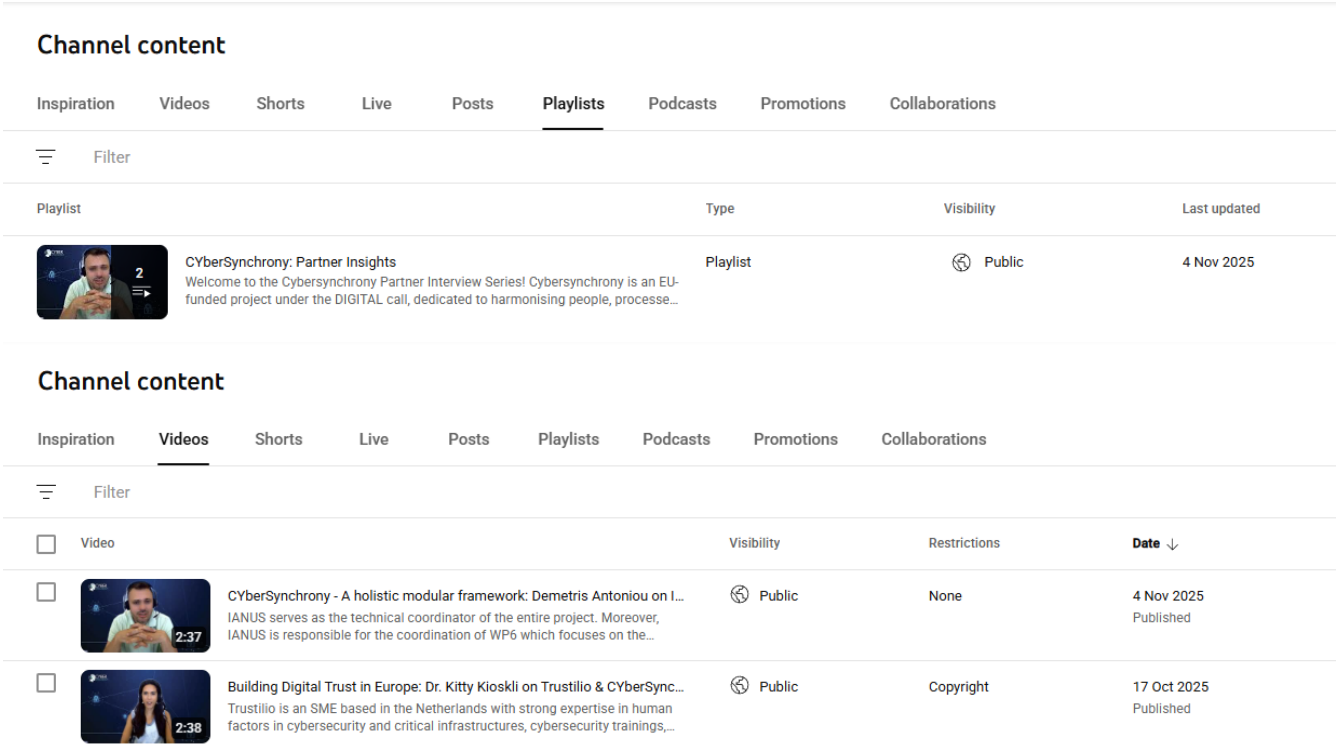

Figure 20. YouTube Channel content (video uploads & playlist).

4.2.3 X-Account

X platform is a fast-paced space for real-time updates, fostering quick and interactive engagement with a global audience in the cybersecurity, and not only, sector. CYberSynchrony's X-account is used to share brief, timely announcements, project news, event highlights, and industry trends while engaging in live conversations and responding to current cybersecurity challenges. With its concise messaging and immediate interactions, CYberSynchrony's X account will help build awareness, spark discussions, and amplify the project's outreach in the digital sphere, making it a vital tool for connecting with both professionals and the broader public in a more dynamic, and immediate manner.

Figure 21. CYberSynchrony's X-Account.

4.3 Newsletters & Emailing Lists

As part of the project's D&C strategy, the CYberSynchrony newsletter plays a key role in keeping stakeholders and the public informed about the latest developments, milestones, and outcomes of the project. Released bi-annually, the newsletter serves as a comprehensive source of information for researchers, industry professionals, policymakers, and other interested parties who want to stay updated on the progress and impact of CYberSynchrony Project.

The project has to date published **two newsletters**, which are freely accessible from the "Newsletters" section of the CYberSynchrony website. The newsletters are built and distributed via Mailchimp, ensuring professional design, reliable delivery, and the ability to track engagement metrics. Each edition serves as a structured communication touchpoint to update stakeholders, such as researchers, industry partners, SMEs, and policy-makers, on the latest project milestones, upcoming events, dissemination activities, and opportunities for engagement. The issues incorporate a mix of content: project highlights (for example participation in conferences and workshops), partner spotlights, and links to multimedia resources and social-media channels. By using this format, the project ensures regular and direct outreach to its distribution list, reinforcing awareness, transparency, and involvement in the project's broader ecosystem. Monitoring of newsletter issuance forms an integral part of the communications KPI framework, tracking publication dates, open and click rates (when available), subscriber growth, and topical relevance. This structured approach helps ensure that the newsletter channel remains aligned with the project's objectives of wide visibility, stakeholder engagement, and sustained communication impact. Other online publishing material can be found on the website here.

4.3.1 Subscription

Subscribing to the CYberSynchrony newsletter is simple and open to all interested individuals and organizations. The subscription process is managed via a Mailchimp [7] account, ensuring a streamlined and secure experience for subscribers. Stakeholders can sign up directly on the CYberSynchrony website by filling out a subscription form (Figure 22), which automatically adds them to the mailing list managed through Mailchimp. This platform allows us to efficiently handle subscriber data, ensuring GDPR compliance while enabling targeted and personalized communication. By subscribing, stakeholders will receive the newsletter directly to their inboxes, ensuring they remain up to date with the project's ongoing activities and plans. Up to date we have 245 total contacts and 226 email subscribers.

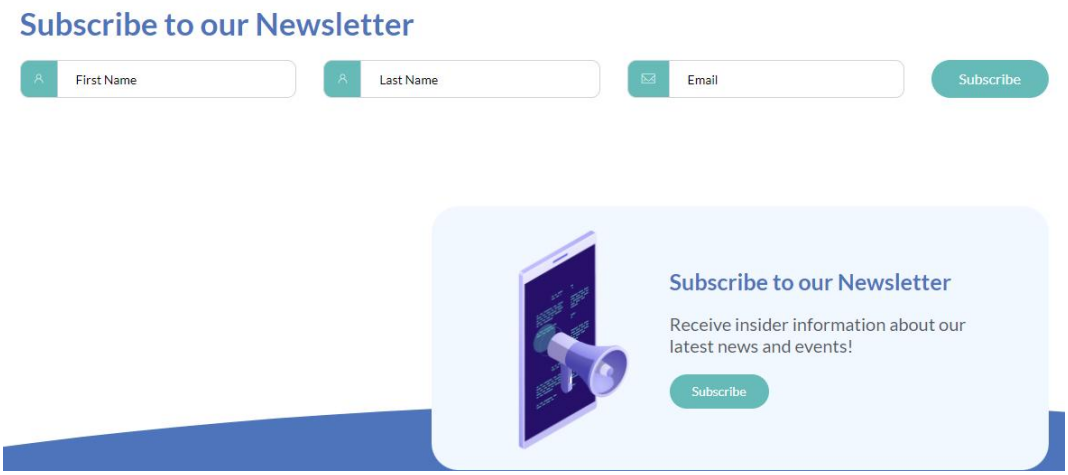

Figure 22. One-step Subscription through CYberSynchrony website: Newsletters - CYberSynchrony .

4.4 Promotional Material

The CYberSynchrony project has developed a range of high-quality promotional materials, including roll-up banners, brochures, flyers, and infographics, which are designed to clearly communicate the project's objectives, activities, and impact. These materials have been used at conferences, workshops, and other dissemination events to enhance visibility and engagement with stakeholders. All four promotional contents are available on the project website, providing easy access for partners, stakeholders, and the broader public. By combining visually appealing design with clear messaging, these materials support the project's outreach efforts, help attract new collaborators, and strengthen the recognition of CYberSynchrony across the European cybersecurity ecosystem.

Figure 23. Promotional material as displayed on the website.

4.5 Multimedia

As part of its communication strategy, the CYberSynchrony project has produced and published two interviews with project partners, providing insights into the project's objectives, technical achievements, and contributions to European cybersecurity. These interviews have been uploaded to the CYberSynchrony YouTube channel, making them widely accessible to stakeholders, researchers, and the public. By offering firsthand perspectives from consortium members, the interviews serve as an engaging tool to highlight the project's impact, foster transparency, and encourage broader engagement with the project's activities. Plans are also in place to complement this content with a high-quality animated promotional video, which will further enhance visual storytelling and outreach to diverse audiences. The preparation to produce an animated video has been initiated by eBOS in M17 and includes specifications documentation (Annex I).

4.6 Public Talks

4.6.1 University Public Events

- **CYberSynchrony Participated in Two Cybersecurity Workshops in Greece, in March 2025**

The CYberSynchrony project participated in two high-impact cybersecurity workshops hosted in Greece in March 2025. These events served as key clustering activities, bringing together leading European projects and cybersecurity stakeholders to address critical sectoral challenges and emerging threats.

- **Workshop on Cybersecurity in Critical Sectors -** *University of West Attica, Athens*

The "Workshop on Cybersecurity in Critical Sectors" was held on March 11, 2025, at the University of West Attica, Department of Informatics and Computer Engineering, Aegaleo Park Campus. As a collaborative initiative among the CyberSecPro, NERO, and CYberSynchrony DEP projects, the workshop attracted significant attention, with over 570 participants, 90% of whom attended in person.

Over the span of six hours, the workshop featured in-depth discussions on the cybersecurity needs and challenges in key sectors such as healthcare, energy, and transportation. The CYberSynchrony partner University of Piraeus Research Center (UPRC) played a central role in the dialogue, sharing insights and contributing to collaborative exchanges aimed at enhancing cyber resilience.

© CYberSynchorny, 2024

Figure 24. Photos taken during the Workshop on Cybersecurity in Critical Sectors.

- **Workshop on "Cybersecurity – Modern Trends and Concerns – The Malware-as-a-Service Ecosystem" –** *University of the Peloponnese, Sparta*

On March 13, 2025, CYberSynchrony participated in a second dynamic event hosted by the Department of Digital Systems at the University of the Peloponnese in Sparta. The workshop, titled: "Cybersecurity – Modern Trends and Concerns – The Malware-as-a-Service Ecosystem", was organized as part of the clustering activities of CyberSecPro, NERO, and CYberSynchrony DEP projects, alongside the Lazarus and SafeHorizon Horizon Europe projects. With over 120 active participants and additional viewers joining online via livestream, the event successfully highlighted current cybersecurity threats and collaborative approaches to counter them. Special thanks to Dimitris Koutras from CYberSynchrony partner Focal Point (FP), whose coordination and dedication were instrumental to the event's success.

These workshops reaffirm CYberSynchrony's commitment to fostering cross-project cooperation and knowledge-sharing across Europe. By actively contributing to high-level discussions and forming synergies with other EU-funded initiatives, the project strengthens its mission to improve the cyber resilience of Europe's critical infrastructures.

Figure 25. Photos taken during the Workshop on "Cybersecurity – Modern Trends and Concerns"

- **Training at the University of Piraeus (13/01 & 04/02/2025)**

The "Human Aspects of Cybersecurity" training targeted postgraduate cybersecurity students, early-career researchers, and young professionals specialising in information security, digital systems, and applied cyber-risk management. The sessions explored human-centric dimensions of cybersecurity, focusing on how behavioural, psychological, cognitive, organisational, and socio-technical factors influence cyber risk exposure and the maturity of defence strategies.

TRUST presented key principles and practical examples covering user behaviour, attacker profiling, psychosocial risk drivers, cognitive biases in decision-making, and the impact of organisational culture on security resilience. Participants engaged in discussions around real-world case studies, emerging threats linked to human vulnerabilities, and the role of trust governance in AI-enabled cyber operations. The sessions also highlighted relevant EU policies and regulatory frameworks, including NIS2, the Cybersecurity Act, and the AI Act, demonstrating how human-factor evidence is increasingly integrated into assurance and compliance practices.

© CYberSynchorny, 2024

Overall, the training contributed to skills development and capacity building among the next generation of cybersecurity professionals, strengthening awareness of the human dimension of security and promoting trust-oriented approaches in practice.

- **TAROT Summer School – For more details "Chapter 3.1.1"**
- **CyberHOT Summer School – For more details "Chapter 3.1.1"**

Figure 26. Roll-up banner and consortium partners showcasing CYberSynchrony at the CyberHOT 2025.

4.6.2 University Open Days

- **CYberSynchrony at University of Piraeus Career Days**

The CYberSynchrony project was represented by partners University of Piraeus Research Center (UPRC) and Focal Point at the Career Days 2025 event, held on 10–11 April 2025 at the University of Piraeus. The event serves as an important platform connecting academia and the professional world, providing students and recent graduates with insights into current job market trends and direct engagement with industry representatives.

During the event, the CYberSynchrony team engaged with over 40 attendees, including students and recent graduates. Through individual discussions and informative sessions, the team presented the project's objectives, expected impact, and its innovative approach to synchronizing cybersecurity responses across sectors. Attendees gained an understanding of the project's contributions to advancing cybersecurity and learned about opportunities to participate in building a safer digital ecosystem.

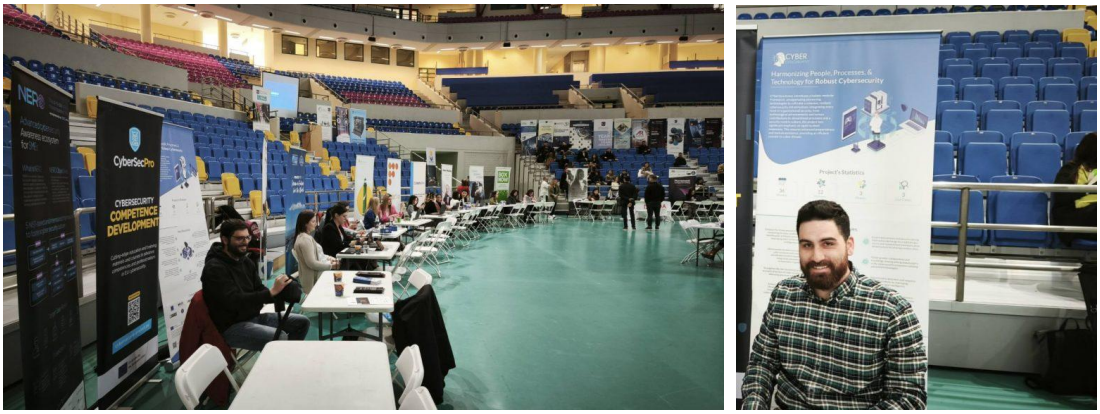

Figure 27. Focal Point representing CYberSynchrony at Career Days 2025 event with roll-up and flyers.

© CYberSynchorny, 2024

4.6.3 Events hosted by local entities and societal stakeholders

- **Cyber Security Winter School 2025 – For more details "Chapter 3.1.1"**
- **Participating in CIE 2025 Conference on Informatics in Education, Piraeus, Greece – For more information "Chapter 3.3"**
- **Presenting CYberSynchrony in the Digital Europe Programme (DEP) InfoDay**

On 9 July 2025, the CYberSynchrony project was featured at the Digital Europe Programme (DEP) InfoDay held in Nicosia, Cyprus, which brought together digital leaders and organisations to discuss Europe's digital policy landscape and share best practices from EU-funded initiatives. The project was presented by eBOS Technologies, represented by Dr. Elisavet Grigoriou and Dr. Charalambos Klitis, who highlighted CYberSynchrony as a holistic, cross-border cybersecurity framework designed to enhance collaboration, compliance, and resilience across EU Member States.

The presentation focused on CYberSynchrony's comprehensive cybersecurity deployment framework, which integrates technical innovation, human-centric processes, and governance models to strengthen Europe's ability to prevent, detect, and respond to cyber incidents. Through its Financial Support to Third Parties (FSTP) mechanism, the project empowers SMEs and public bodies to improve their cyber resilience and implement best practices in line with European standards. CYberSynchrony's contribution was recognised during the InfoDay for its success in bridging the gap between research innovation and large-scale deployment, promoting secure-by-design principles and fostering coordinated cybersecurity responses across Europe.

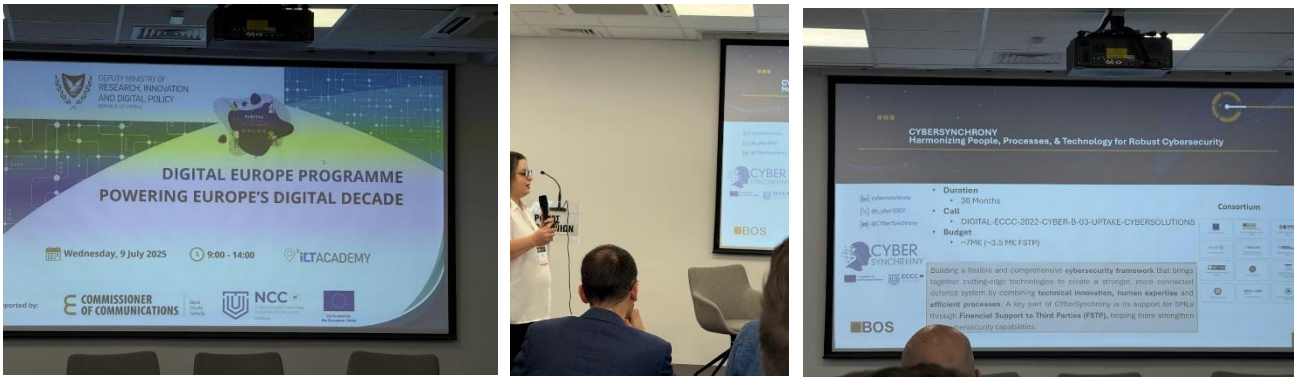

Figure 28. Dr. Elisavet Grigoriou presenting CYberSynchrony at the DEP InfoDay – Cyprus.

© CYberSynchorny, 2024

5 Impact (Analytics)

The data analytics provide an in-depth view of how users are interacting with the website and social media posts, offering valuable insights into visitor behaviour, traffic sources, and engagement patterns. By analyzing key metrics such as session duration, page views, referral sources, and geographic distribution, we can assess the effectiveness of the website in reaching and engaging its audience. The insights derived from the M1-12 analysis, have informed the prioritisation of D&C activities during M13–M18, with resources increasingly directed toward channels that show higher engagement or that stakeholders identify as most useful through surveys and event feedback. Analytics also guide adjustments to content formats and posting frequency, ensuring continuous optimisation. In parallel, clustering targets are selected based on thematic alignment, complementary expertise, and demonstrated relevance within the EU cybersecurity ecosystem, allowing for transparent and methodical collaboration building. Regular monitoring ensures that the digital ecosystem remains an effective platform for disseminating information, attracting new audiences, and sustaining meaningful engagement.

5.1 Google Analytics (Website)

The CYberSynchrony project website has experienced consistent traffic throughout the reporting period, with a total of 3.8K active users, all of whom were new users (Figure 29). The average engagement time per user is approximately 1minute, however there are several visitors exploring the website between 3 to 10 minutes, indicating that visitors are actively exploring the website content, though there is potential to further enhance engagement with more interactive or targeted content. Analysis of the traffic trends over time shows several notable spikes in activity. The most significant peak occurred around early July 2025, suggesting a direct correlation with specific dissemination activities, such as webinars, workshops, or public events that were promoted during this period. Smaller spikes earlier in the year and around October also indicate periods of increased user interest, likely linked to targeted communication campaigns or the release of new content.

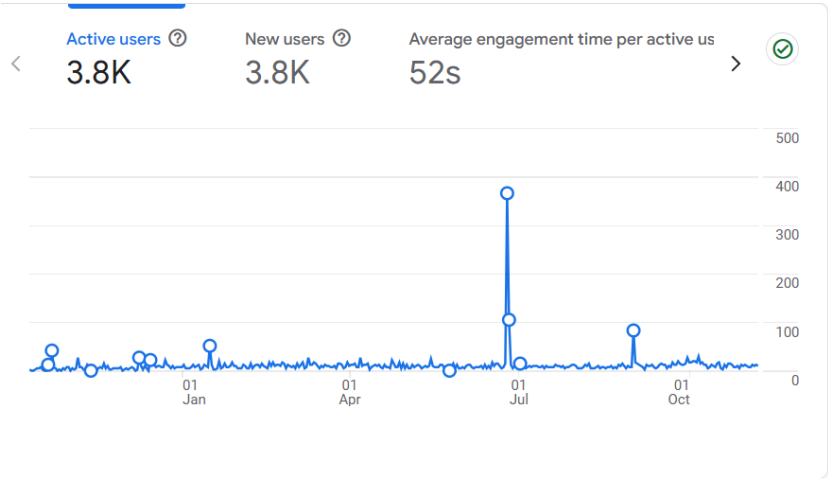

Figure 29. Google Analytics for the period October 2024 to November 2025, presenting the visitors of the website.

Figure 30. Google Analytics for the period October 2024 to November 2025, presenting the time spent on the website by visitors.

Most of the visitors are coming from direct links (~3,000) to the website, indicating that a significant portion of the audience is already familiar with the platform or has been specifically directed to it. However, there is also a noticeable number of users arriving via referrals (~500) from other websites, social media accounts, or external links. Interestingly, these referral users tend to engage more deeply with the website, spending an average of 3 minutes and 36 seconds per session. In comparison, users arriving through organic search spend an average of 1 minute and 33 seconds on the site, which, while shorter than referral users, still exceeds the average time spent by direct visitors (Figures 30-31). This suggests that users who discover the website through curated or context-specific channels may be more interested in exploring its content in depth.

Additionally, the website has attracted 166 returning users, indicating a growing base of repeat visitors who find ongoing value in its content. Geographically, most visitors originate from the United States, reflecting a strong engagement within the primary target region. Nevertheless, there is a notable presence of visitors from Greece, Ireland, the Netherlands, Cyprus, Germany, and Italy (Figure 32), highlighting the website's reach and relevance to an international audience.

Overall, these insights confirm that the website continues to serve as an effective channel for disseminating project outputs and engaging a diverse community of users. Regular monitoring of user behaviour and engagement metrics will be critical for optimizing content delivery, identifying high-impact pages, and enhancing the overall user experience. By understanding the preferences and interaction patterns of different user segments—direct, referral, and organic—future content strategies can be tailored to maximize both reach and engagement.

		First user prim...Channel Group) +	Total users	↓ New users	Returning users	Average engagement time per active user
☑		Total	3,820 100% of total	3,827 100% of total	166 100% of total	52s Avg 0%
☑	1	Direct	3,094 (80.99%)	3,108 (81.21%)	80 (48.19%)	23s
☑	2	Referral	502 (13.14%)	502 (13.12%)	11 (6.63%)	3m 36s
☑	3	Organic Search	205 (5.37%)	201 (5.25%)	68 (40.96%)	1m 33s
☑	4	Organic Social	19 (0.5%)	16 (0.42%)	7 (4.22%)	18s

Figure 31. Engagement Analytics.

© CYberSynchorny, 2024

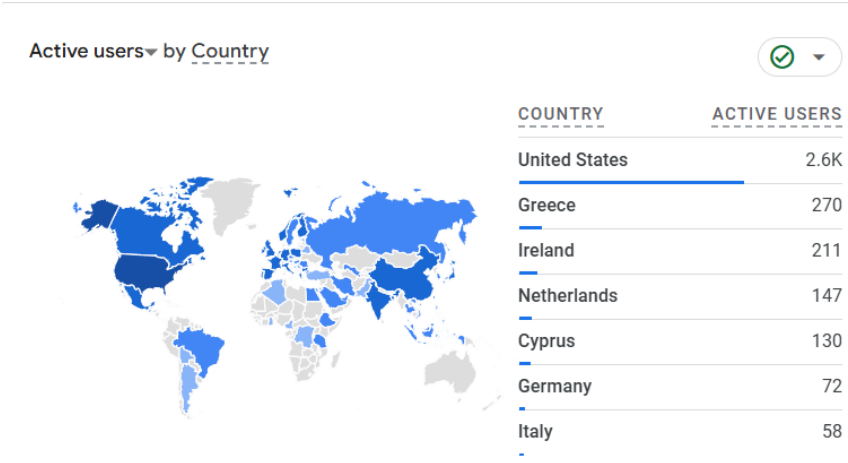

Figure 32. Map of visiting countries analytics.

5.2 LinkedIn

The LinkedIn analytics provide a comprehensive overview of the performance and reach of our professional presence on the platform. By examining key metrics such as follower growth, post engagement, impressions, and demographic breakdowns, we can gain valuable insights into how effectively our content resonates with the target audience. These analytics not only highlight trends in audience behaviour and interaction but also inform strategic decisions to enhance visibility, strengthen community engagement, and optimize content for maximum impact. Understanding these patterns allows for a more data-driven approach to professional networking and ensures that our LinkedIn activities continue to support broader organizational objectives.

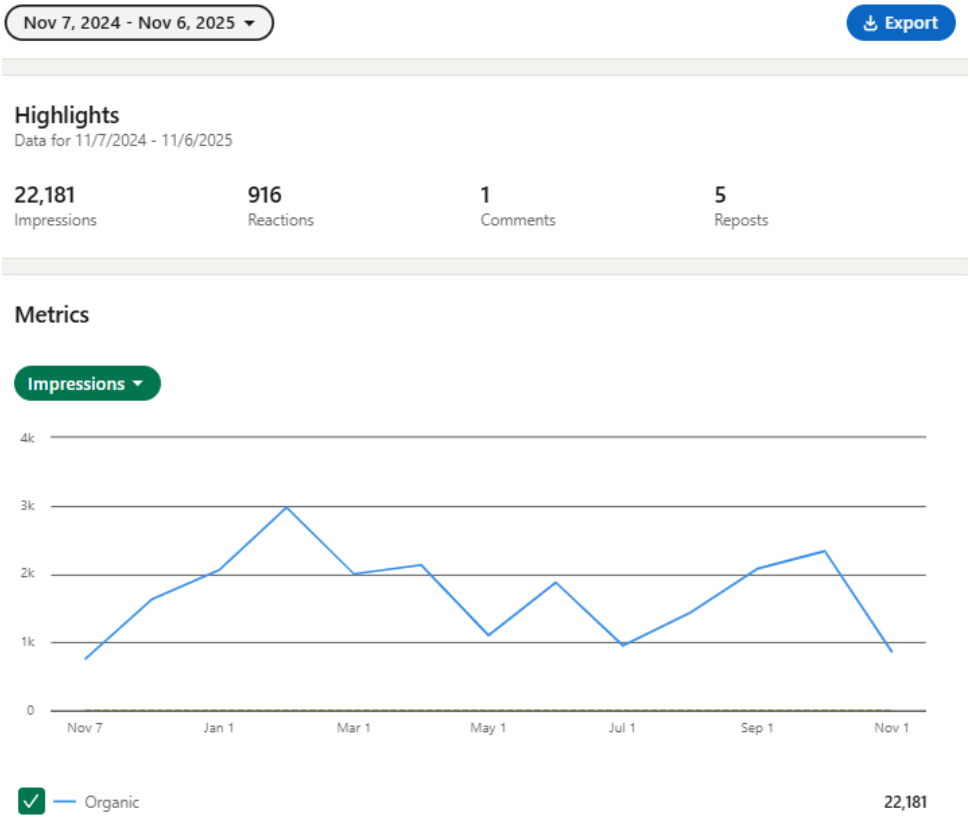

Figure 33. LinkedIn analytics for Impression metrics (Nov 2024-Nov 2025)

© CYberSynchorny, 2024

Between November 2024 and November 2025, the LinkedIn page achieved a total of 22,181 impressions, accompanied by 916 reactions, demonstrating steady visibility and engagement over the course of the year. When broken down monthly, the page averaged approximately 2,000 impressions per month, with individual months ranging from 1,000 to 3,000 impressions. This variation reflects periods of higher content activity as well as fluctuations in audience interaction, which can inform timing and content strategy for future posts (Figure 33).

In terms of reach, the content was seen by an average of 750 members each month, with monthly figures ranging from 250 to 1,250. This indicates that the page is successfully attracting both existing followers and new viewers and highlights the potential for expanding the audience through targeted content and engagement initiatives. Click-through activity also showed meaningful engagement, with posts receiving an average of 200 clicks per month, fluctuating between 50 and 450 clicks depending on the content type and relevance. Meanwhile, reactions) such as likes, celebrates, and other forms of engagement (averaged 60 per month, with peaks of up to 140 in certain months, suggesting that some posts resonated particularly well with the audience.

Overall, these analytics indicate that the LinkedIn page is performing effectively as a professional communication channel. The consistent reach, engagement, and interaction demonstrate that the content is connecting with the intended audience and fostering meaningful professional engagement. Regular monitoring of these metrics will allow for further optimization of content strategies, ensuring that posts continue to attract attention, encourage interaction, and maximize the overall impact of the page over time. By analysing monthly trends, engagement patterns, and high-performing content, the organization can refine its LinkedIn strategy to strengthen its online presence, reach new audiences, and maintain a vibrant professional community.

5.3 Mailchimp

As of November 2025, the Mailchimp mailing list consists of a total of 245 contacts, including 226 active email subscribers (Figure 34). Over the reporting period, two newsletter issues were released. The first newsletter achieved a strong engagement rate, with approximately 50% of recipients opening the email and 17% clicking on included links. The second newsletter, however, experienced a lower engagement rate, with 37% opens and 0.8% clicks (Figure 35). Analysis of the click activity indicates that the majority of interactions were directed toward the project's social media accounts and website, suggesting that readers are particularly interested in engaging with the project through external channels.

Overall, these figures provide useful insight into the performance of the email communication channel. While the initial newsletter demonstrated high engagement, the drop in the second issue highlights the importance of continuous optimization of content, timing, and link placement to maintain audience interest. Monitoring these metrics over time will help identify patterns in subscriber behavior, refine messaging strategies, and enhance the effectiveness of future campaigns in keeping the community informed and engaged.

© CYberSynchorny, 2024

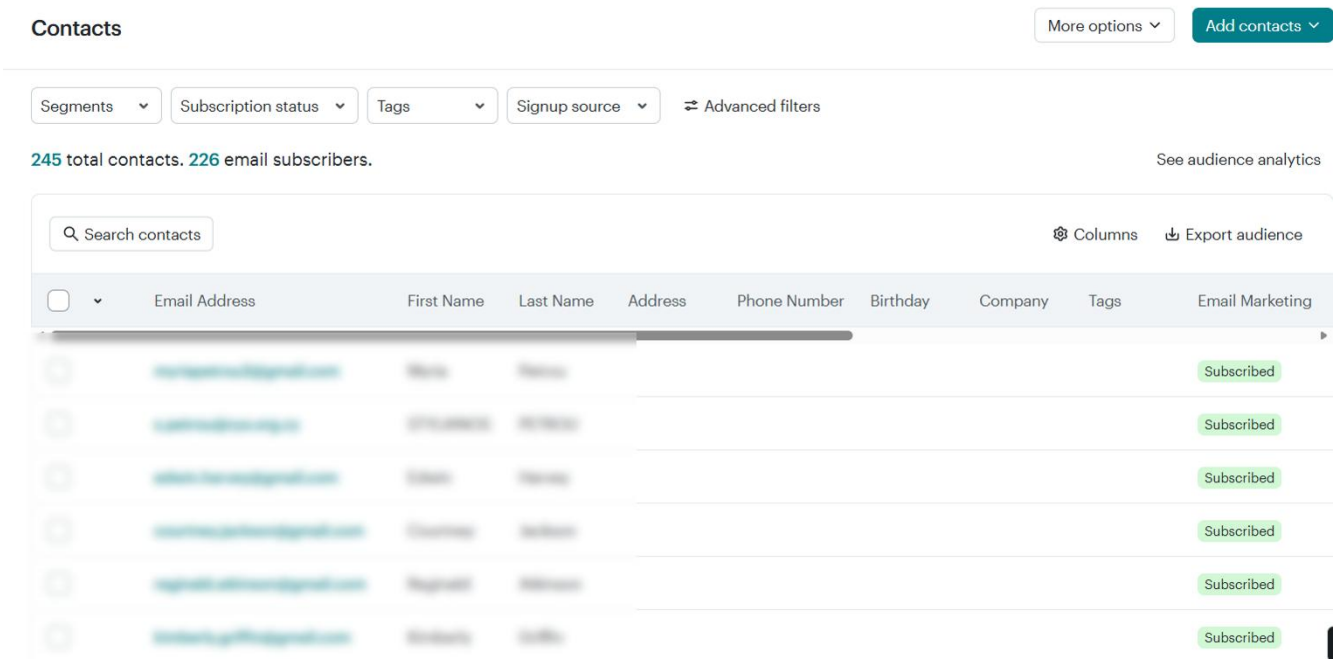

Figure 34. Screenshot of Mailchimp contact list (blurred for GDPR).

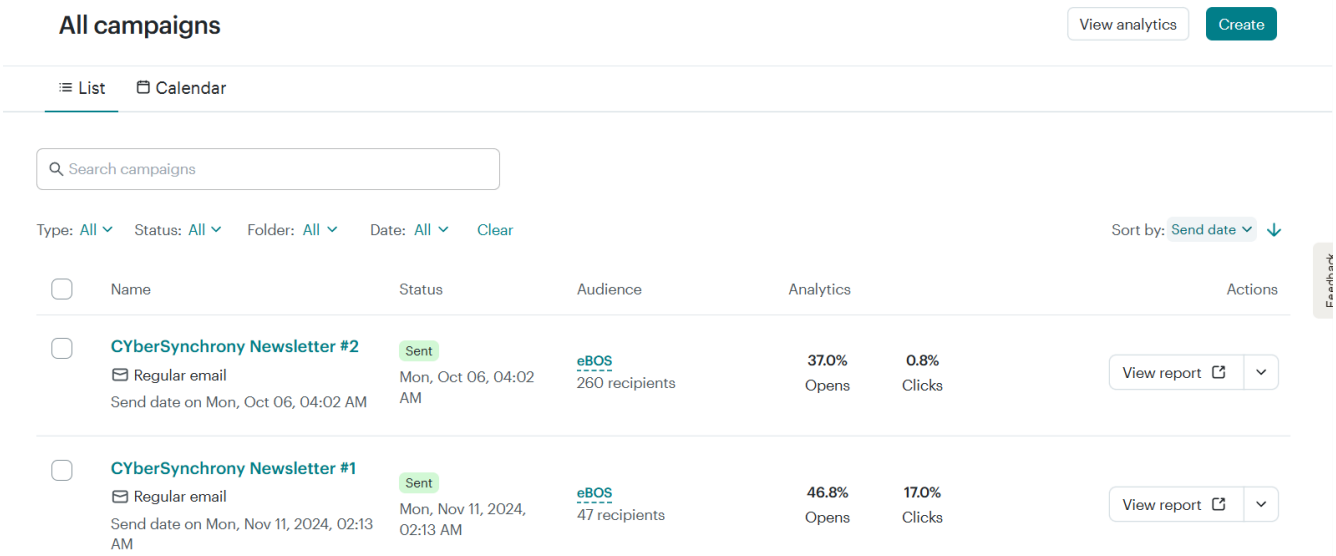

Figure 35. List of campaigns (Newsletters) released and their performance analytics.

© CYberSynchorny, 2024

6 Clustering Activities

Throughout the reporting period, CYberSynchrony actively engaged in a series of high impact clustering activities, strengthening collaboration and knowledge exchange within the European cybersecurity ecosystem. CYberSynchrony has actively participated in the official launch of the CRACoWi Project (Cyber Resilience Act – Compliance Wizard), which took place during a two-day Kick-off Meeting and press conference in Athens. Alos, CYberSynchrony took part in the Cyber Security Winter School 2025 in Lisbon, from 20 to 25 January. Partners from TRUST, UPRC, FP, and MAG, contributed through technical sessions and collaborative discussions on critical topics, including the risks of vulnerable binaries and the configuration of intrusion detection systems. This participation reinforced CYberSynchrony's commitment to advancing cybersecurity skills, promoting innovation, and clustering with other EU-funded projects such as CyberSecPro to accelerate progress in cybersecurity education and practice.

Also, the project participated in the NERO Webinar "From Risk to Resilience: Navigating the Cybersecurity Solutions Marketplace" on 29 January 2025, where Dr. Violeta Vasileva (Gruppo Maggioli) presented the project's objectives, expected impacts, and use cases. This event, which featured contributions from multiple European initiatives, promoted cooperation and the sharing of best practices among projects such as NERO, CyberSuite, and CyberSecPro, fostering synergies in cybersecurity research and resilience building.

In March and May 2025, CYberSynchrony continued to strengthen cross-project collaboration through its involvement in cybersecurity workshops in Greece and a dedicated R&D clustering session during CyberHOT 2025 in Crete. The workshops, organised in cooperation with projects such as CyberSecPro and NERO, focused on cybersecurity in critical sectors and the growing threat of Malware-as-a-Service. The CyberHOT 2025 session brought together 17 EU-funded initiatives, where CYberSynchrony presented its technical vision, modular architecture, and strategies for engaging SMEs through its upcoming open call. These activities collectively enhanced the project's visibility, supported cooperation across Europe's cybersecurity landscape, and reinforced its mission to improve the resilience of critical infrastructures.

6.1 Performed

- **CYberSynchrony participated in the NERO Webinar "From Risk to Resilience: Navigating the Cybersecurity Solutions Marketplace" – For more information "Chapter 3.1.2"**
- **CYberSynchrony participated at the Cyber Security Winter School 2025 – For more information "Chapter 3.1.1"**
- **Dedicated R&D clustering Session during the CyberHOT 2025: Advancing Collaboration and Cybersecurity Training in Crete – For more information "Chapter 3.1.1"**
- **CYberSynchrony Joins the CRACoWi Project Kick-off Event in Athens**

CYberSynchrony has actively participated in the official launch of the CRACoWi Project (Cyber Resilience Act – Compliance Wizard), which took place during a two-day Kick-off Meeting and press conference in Athens. Organized by ITML, the project coordinator, the event marked the beginning of an ambitious initiative funded under the Digital Europe Program (DEP) and supported by the European Cybersecurity Competence Centre (ECCC).

The CRACoWi Project is Simplifying Cybersecurity Compliance: At the heart of the project is the development of the Compliance Wizard – a digital tool tailored for small and medium-sized enterprises (SMEs), manufacturers, and distributors. The Compliance Wizard will simplify and streamline the process of complying with the EU's Cyber Resilience Act (CRA), which establishes new cybersecurity requirements for products and services in the digital space. The tool aims to automate essential tasks such as compliance assessments, the generation of required documentation, and guidance on obtaining cybersecurity certifications. By facilitating these processes, CRACoWi ensures that businesses can seamlessly integrate and maintain cybersecurity standards throughout their product lifecycles, helping them meet the challenges posed by new regulatory frameworks with ease and efficiency. CYberSynchrony's Role in CRACoWi: As part of its clustering activities, CYberSynchrony contributes to

© CYberSynchorny, 2024

the CRACoWi project's mission of enhancing cybersecurity resilience across Europe. CYberSynchrony is clustering with this innovative project, working alongside leading European institutions and organizations to bolster cybersecurity resilience for businesses across the EU.

Figure 36. CYberSynchrony presentation during the official launch of the **CRACoWi Project** (Cyber Resilience Act – Compliance Wizard) at the kick-off.

- **1st CyberSuite Hackathon, at JOIST Innovation Park, Larissa, Greece**

Our partner from TRUST, Dr. Leandros Maglaras, participated in the 1st CyberSuite Hackathon that took place on the 31st of October 2025 at the JOIST Innovation Park, Larissa, Greece. This event brought together experts, researchers, and industry professionals to explore key challenges in cybersecurity vulnerability assessment, code analysis, phishing campaigns and many other emerging challenges in the cybersecurity ecosystem. During the hackathon Leandros had the chance to test some of the tools created from the CyberSuite consortium and provide his feedback regarding those tools and the Hackathon itself. This was a nice opportunity to advise on the progress of the project but on the same time to discuss about the work that is being made in the CYberSynchrony project.

Figure 37. Dr. Leandros Maglaras at the 1st CyberSuite workshop.

During the discussions with experts from the CyberSuite consortium, Leandros highlighted the objectives, expected impacts, and three core use cases (UCs) driving CYberSynchrony's research and implementation (Figure 37). This event facilitated a valuable clustering activity, strengthening connections and promoting knowledge exchange about related initiatives between CyberSuite, and CYberSynchrony, enhancing the collective impact of European cybersecurity research.

© CYberSynchorny, 2024

6.2 Planned

Building on the strong collaborations established during the reporting period, CYberSynchrony will continue its clustering efforts through active participation in upcoming European cybersecurity events and initiatives throughout the next reporting period. CYberSynchrony will continue participating in **joint clustering sessions** with projects such as **CyberSecPro, NERO, and CRACoWi**, focusing on topics including AI-driven threat detection, cyber resilience for SMEs, and the alignment of research outputs with EU policy objectives. These events will serve as a platform to strengthen ties with other projects, explore future cooperation opportunities, and enhance the visibility of CYberSynchrony within the European cybersecurity ecosystem.

In early 2026, CYberSynchrony will continue to reinforce its engagement with the European cybersecurity ecosystem through a dedicated joint webinar with the COBALT Horizon project, titled **"Roadmap to a European Trusted Cyber Ecosystem: Tools, Policies & Certifications"** (tentatively scheduled for March 2026). The event will bring together representatives from both initiatives and key contributors from the certification and policy domains, including TÜV and other European cybersecurity actors. The session will feature presentations by COBALT Horizon Project and CYberSynchrony, followed by technical showcases of the COBALT Certification Platform and the CYberSynchrony Modular Platform. Participants will gain insights into how advanced threat intelligence, mutual-assistance exercises, and certification schemes such as EUCS and EUCC can converge into a unified, testable, and scalable European cyber trust architecture.

This collaborative event will not only foster cross-project knowledge exchange but also strengthen alignment with EU cybersecurity certification frameworks and policy objectives. By bridging policy, technical, and operational perspectives, the webinar aims to deliver actionable insights for industry, SMEs, and public stakeholders, supporting the creation of a more trusted and resilient European cyber ecosystem. The COBALT Horizon collaboration represents the next step in CYberSynchrony's clustering strategy, deepening cooperation with Horizon Europe and DEP-funded projects while promoting interoperability and shared innovation across the European cybersecurity community.

© CYberSynchorny, 2024

7 Conclusions

The deliverable D9.3 outlines the overall Dissemination and Communication activities performed following the strategy that was defined in D9.1, to ensure a broad dissemination of CYberSynchrony's project outcomes. It also includes dedicated chapters on the tools, activities, and key performance indicators (KPIs) monitoring for the project's dissemination and communication, along with the achieved KPIs and data analytics of the social media platforms. These chapters outline the methods and metrics used to maximize outreach, engage stakeholders, and ensure effective communication of the project's outcomes.

The D&C, and clustering activities carried out within the CYberSynchrony project have successfully ensured that project outputs are widely shared, understood, and utilized by relevant stakeholders. Through a structured strategy combining events, publications, social media, and targeted engagement with academic, industrial, and societal communities, the project has maximized visibility and promoted knowledge transfer.

The analysis of impact metrics, including website analytics and social media engagement, demonstrates the effectiveness of the project's communication efforts, while clustering activities have fostered collaboration and synergies with complementary initiatives. The combined approach of dissemination and communication has strengthened the project's presence within the research community and among external stakeholders, ensuring that the results are both accessible and actionable.

For the upcoming months, M25–M36, activities will build on these insights by increasing the use of high-performing channels identified in the first reporting periods, coordinating partner-led campaigns around key project milestones, and intensifying clustering actions with EU cybersecurity networks. Partners will use the reported results to refine their communication activities, adjust audience targeting, prioritise formats with proven engagement, and integrate analytics more systematically when planning upcoming tasks such as events, publications, and community outreach. The remaining KPIs are considered achievable, as the planned activities include expanded communication campaigns, broader stakeholder mobilisation through workshops and external events, and closer alignment with established EU initiatives (all of which directly support the outstanding indicators).

This continued effort will sustain project visibility and strengthen CYberSynchrony's scientific, industrial, and societal impact throughout the final project phase and beyond. CYberSynchrony's efforts provide robust efforts for promoting innovation, collaboration, and knowledge exchange in the cybersecurity sector.

© CYberSynchorny, 2024

8 References

1. Communication, dissemination & exploitation what is the difference and why they all matter, European Research Executive Agency, 16 June 2023, PDF Accessed November 2024 [Online]
2. Webinar session: "Dissemination & Exploitation in Horizon Europe", European Commission, 9 June 2021, YouTube, Accessed November 2024 [Online]
3. https://en.wikibooks.org/wiki/GUI_Design_Principles , Accessed October 2024 [Online]
4. https://wordpress.org/about/ , Accessed September 2024 [Online]
5. Your WordPress.com Site and the GDPR – WordPress.com Support, Accessed October 2024 [Online]
6. Analytics | Home (google.com) , Accessed October 2024 [Online]
7. https://mailchimp.com/, Accessed November 2024 [Online]

© CYberSynchorny, 2024

Annex I – Multimedia: Initiation of the production of a promo animated video.

CREATIVE BRIEF -DRAFT v0.1

VIDEO

Client / Client contact information: EK, eBOS Technologies Ltd.

Project name and description: CYberSynchrony

Prepared by: EK

1. PROJECT OVERVIEW

CYberSynchrony introduces a holistic modular framework, amalgamating pioneering technologies to cultivate a cohesive, resilient cybersecurity infrastructure. Integrating every facet of organizational security, from technological advancements and human contributions to streamlined processes and a security-centric culture, the project lays significant emphasis on rapid incident responses. This ensures enhanced preparedness and mutual assistance, providing an efficient counter to cyber threats. The system incorporates advanced threat intelligence platforms and analytics tools, ensuring top-tier threat assessment, robust risk monitoring, and early incident detection. Furthermore, it champions crossborder collaboration using secure communication channels, promoting synchronized actions and information exchange among Member States.

2. OBJECTIVES

Project Promo, awareness on the tools and modules developed within CYberSynchrony

3. TARGET AUDIENCE

SMEs, companies related to cybersecurity, based in EU area, NIS2 companies. Companies that seek to enhance their cybersecurity strategies through trusted tools.

Persona: – IT Security Manager at an EU-based SME, seeking trusted, NIS2-compliant tools to strengthen cybersecurity while ensuring regulatory compliance and operational efficiency. Focuses on reliable, easy-to-integrate solutions that protect data and reduce risk.

4. KEY MESSAGE

“Protect your business with trusted, EU-compliant cybersecurity solutions designed to keep you ahead of threats and aligned with NIS2 regulations.”

Focus on credibility, compliance, and measurable impact through implementing, trialing CYberSynchrony modules.

5. CALL TO ACTION

Feel the need of protecting their company (SME) by using CYberSynchrony Tools and eager to learn more about cybersecurity through our gamified tools for cybersecurity awareness.

6. TONE & STYLE

Professional with a trustworthiness tone

(e.g. cinematic, emotional, bold, professional, fun, friendly, energetic, premium) Please share any reference links to videos you like or dislike.

© CYberSynchorny, 2024

7. VISUAL DIRECTION

Describe any initial ideas for visuals. Are there specific locations, colours, environments, or stylistic elements that inspire this project?

8. WHERE WILL IT BE WATCHED?

List platforms or placements (e.g. website**, YouTube**, Instagram, TikTok, LinkedIn, TV, events, ads)

9. DELIVERABLES & FORMATS

Which final versions do you need?

- Full edit: 120 min clip
- Aspect ratios needed: 16:9
- File formats: mp4

10. TALENT, VOICE & SCRIPT

N/A

11. MANDATORY ELEMENTS

Please list any **non-negotiables** (logo, brand colours, music style, disclaimers, legal text, tagline, do-not-use instructions)

Logo, brand colours, disclaimers, EU funding statement, do not use any material related to the producer/company.

12. ASSETS & AI USAGE

Will you provide any brand assets? Logo, fonts, colour codes
Are AI tools (voice, images, enhancement) allowed or restricted? Allowed – to be discussed

13. ACCESSIBILITY REQUIREMENTS

Do you need captions, translations, or accessibility-friendly design?

If auto captions in YouTube works with the video then we are good.

14. SUCCESS METRICS

>1000 views, >15 interesetd customers/ pilot testers, >2 press coverage

15. TIMELINE & APPROVALS

When would you like to start and when is the deadline? March 2026 – end June 2026
How many people will approve the project? - Project Coordinator, D&C Manager, Technical Manager (3)

How many revision rounds? - It depends on the given work, until reaching the desired quality and content satisfaction.

16. BUDJET

<5000 EU

© CYberSynchorny, 2024

Annex II – D&C Tracker Tool

Journal publications in peer reviewed Journals

KPI >6

Number	Type of PID (repository)*	PID (publisher version of record)*	Type of publication*	Link to publication (to be completed only if DOI not available)	Title of the scientific publication*	Authors*	Title of the Journal or equivalent	ISSN or eISSN*	Publisher*	Month of publication	Year of publication	Was the publication available in open access through the repository at the time of publication*	Peer-reviewed*	PID of Book	Book title
example	DOI	10.1109/TMC.2023.3254888	Article in Journal	Fair and Scalable Orchestration of Network and Compute Resources for Virtual Edge Services	Fair and Scalable Orchestration of Network and Compute Resources for Virtual Edge Services	S. Tripathi, C. Puligheddu, S. Premsankl, A. Garcia-Saavedra, C. Chiasserini	IEEE Transactions on Mobile Computing		1536-1233	IEEE	2024	yes	yes		
1	DOI	https://doi.org/10.54941/ahfe1005635	Article in Conference	https://openaccess.cms-conferences.org/publications/book/978-1-964867-35-6/article/978-1-964867-35-6_73	Optimizing AI System Security: An Ecosystem Recommendation to Socio-Technical Risk Management	K. Kioskli, A. Ramfos, S. Taylor, L. Maglaras, R. Lugo	AHFE International Conference 2024 (Hawaii Edition)	2771-0718	AHFE Open Access Series	45623	2024	yes	yes	NA	NA
2	DOI	https://doi.org/10.3390/electronics14030486	Article in Journal	https://www.mdpi.com/2079-9292/14/3/486	A Practical Human-Centric Risk Management (HRM) Methodology	K. Kioskli, E. Seralidou, N. Polemi	Electronics	2079-9292	Electronics	Jan	2025	yes	yes	NA	NA
3	DOI	https://doi.org/10.1007/s10207-025-01009-z	Article in Journal	https://link.springer.com/article/10.1007/s10207-025-01009-z?utm_source=rct_congratemail&utm_medium=email&utm_campaign=oa_20250310&utm_content=10.1007%2Fs10207-025-01009-z#citeas	A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain	Kioskli K, Grigoriou E, Islam S, Yiorkas A, Christofi L, Mouratidis M	International Journal of Information Security	2147-0030	Springer	March	2025	yes	yes	NA	NA
4	DOI	https://doi.org/10.1007/978-3-031-93714-8_10	Article in Conference	https://link.springer.com/chapter/10.1007/978-3-031-93714-8_10	End-to-End Encryption: Technological and Human Factor Perspectives.	Maglaras & Kioskli	In: Schmorrow DD, Fidopiastis CM (eds) Augmented Cognition. HCII 2025. Lecture Notes in Computer Science, 15778. Springer, Cham	NA		May	2025	yes	yes	NA	NA
5	DOI	https://doi.org/10.1109/EDUCON63131.2025.11016133	Article in Conference	https://ieeexplore.ieee.org/document/11016133	Cybersecurity Certification for Professional Training: An Overview	D. Kallergis, T. Karvounidis, K. Kioskli and C. Douligeris	2025 IEEE Global Engineering Education Conference (EDUCON)	NA	IEEE	June	2025	yes	yes	NA	NA
6	DOI	https://doi.org/10.34190/ecrws.24.1.3369	Article in Conference	https://papers.academic-conferences.org/index.php/ecrws/article/view/3369	Implementing the European Cybersecurity Skills Framework (ECSF): A Case Study of EU Innovation Projects	Rathod, Kioskli, Rajamaki	the European Conference on Cyber Warfare and Security (ECCWS)	NA		June	2025	yes	yes	NA	NA
	Same KPI achieved														
7	DOI	https://doi.org/10.34190/ecrws.24.1.3766	Article in Conference	https://papers.academic-conferences.org/index.php/ecrws/article/view/3766	Proposal of Harmonising Cybersecurity Professional Education and Training (CPET) in the European Union (EU): Exploratory Study	Rathod, Polemi, Rajamaki	the European Conference on Cyber Warfare and Security (ECCWS)	NA		June	2025	yes	yes	NA	NA
8	DOI	10.54941/ahfe1006136	Article in Conference	https://openaccess.cms-conferences.org/publications/book/978-1-964867-44-1/article/978-1-964867-44-1_8	Human Factors and Strategic Approaches in Cybersecurity: Threats for Critical Infrastructures in NIS2 Domains	Kioskli, Maglaras, Fotis, Varsuchas	In: Abbas Moallem and Kitty Kioskli (eds) Human Factors in Cybersecurity. AHFE (2025) International Conference. AHFE Open Access, vol 168. AHFE International, USA	NA		July	2025	yes	yes	NA	NA