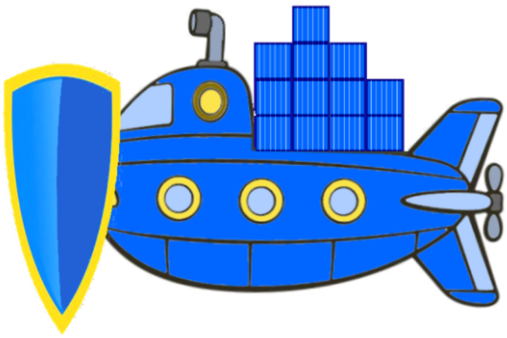


CyberNEMO

End-to-end CYBERsecurity to NEMO meta-OS

D6.5 Dissemination, Standardization &Communities Liaison

STATUS	FINAL	DUE DATE	31/03/2025
VERSION	1.0	DELIVERY DATE	31/03/2025

WORKPACKAGE	6	DOCUMENT	D6.5
LEAD PARTNER	ECL	DISSEMINATION LEVEL	PU
CONTRIBUTING PARTNERS	ALL	REVIEWING PARTNERS	INTRA
			UPAT
KEYWORDS	Stakeholders, Communication, Dissemination, Standardization, Liaison, Social Media, Community Building, Open Source		

© Copyright by the CyberNEMO Consortium

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101168182.



DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.
This document may contain material, which is the copyright of certain CYBERNEMO consortium parties, and may not be reproduced or copied without permission. All CYBERNEMO consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.
Neither the CYBERNEMO consortium as a whole, nor a certain party of the CYBERNEMO consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

	Participant organisation name	Short	Country
01	SYNELIXIS SOLUTIONS SA	SYN	EL
02	DNV AS	DNV	NO
03	THALES SIX GTS FRANCE SAS	TSG	FR
04	ENGINEERING - INGEGNERIA INFORMATICA SPA	ENG	IT
05	NETCOMPANY-INTRASOFT SA	INTRA	LU
06	SIEMENS SRL	SIEM	RO
07	MAGGIOLI SPA	MAG	IT
08	SPACE HELLAS SA	SPACE	EL
11	UNPARALLEL INNOVATION LDA	UNP	PT
12	TELEFONICA INNOVACION DIGITAL SL	TID	ES
13	OTE SA	OTE	EL
14	ASM TERNI SPA	ASM	IT
15	ENTERSOFT SA	ESOFT	EL
16	MEDITCINSKY UNIVERSITET-PLOVDIV	MUP	BG
17	SORBONNE UNIVERSITE	SU	FR
18	UNIVERSIDAD POLITECNICA DE MADRID	UPM	ES
19	RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN	RWTH	DE
20	PANEPISTIMIO PATRON	UPAT	EL
21	UNIVERSIDAD CARLOS III DE MADRID	UC3M	ES
22	ECLIPSE FOUNDATION EUROPE GMBH	ECL	DE
23	SPHYNX TECHNOLOGY SOLUTIONS AG	STS	CH
24	CYBERSOCIAL LAB SRL IMPRESA SOCIALE	CSL	IT
25	XGILITY LIMITED	XGL	IE

ACKNOWLEDGEMENT

This document is a deliverable of CYBERNEMO project. This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101168182.
The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

Document History

Version	Date	Contributor(s)	Description
V0.1	18/11/2024	Rosaria Rossini ECL	ToC
V0.2	21/02/2025	Wafa Ben Jaballah TSG, Luigi Briguglio (CSL), Clio Beruete (UPM)	Contribution to all sections
V0.3	14/03/2025	Vasilis Megalooikonomou (UPAT)	Contribution
V0.4	14/03/2025	Rosaria Rossini ECL	Finalizing
V0.5	17/03/2025	Review	INTRA and UPAT
V0.6	21/03/2025	Wafa Ben Jaballah (TSG)	Refine the document following reviewers' feedback
V0.7	21/03/2025	Clio Beruete (UPM)	Refine the document following reviewers' feedback
V0.8	22/03/2025	Rosaria Rossini (ECL)	Refine the document following reviewers' feedback
V0.9	31/03/2025	Rosaria Rossini (ECL)	Preparing for submission
V1.0	31/03/2025	Artemis Voulkidis, Andreas Papadakis (SYN)	Document finalised and ready for submission

Please note that although the deliverable has been available on the 31st of March, submission was not possible due to technical issues of the ECAS continuous reporting data platform. The issue was escalated to the helpdesk and the PO was promptly updated. The issue was resolved on the 4th of April, and the deliverable was submitted.

Document Reviewers

Date	Reviewer's name	Affiliation
21/03/2025	Dimitrios Skias	INTRA
21/03/2025	Vasillis Megalooikonomou	UPAT

Table of Contents

DISCLAIMER 2
ACKNOWLEDGEMENT 2
Document History 3
Document Reviewers 3
Table of Contents 4
List of Figures 5
List of Tables 5
List of Acronyms and Abbreviations 6
Executive Summary 7
1 Introduction 8
1.1 Relation to other activities 8
1.2 Document overview 8
2 Dissemination & Communication Plan 9
2.1 Dissemination & Communication Strategy and Phases 9
2.2 CyberNEMO Dissemination and Communication 10
2.2.1 Stakeholder analysis 10
2.2.2 Social Media Dissemination 11
2.2.3 Online Channels 11
2.2.4 Participation to events 15
3 European CI security policy & Standardization 17
3.1 Identification of main standards, alliances and associations for CyberNEMO 17
3.2 CyberNEMO in European CI security policy 21
4 Open Source Ecosystem and Community Building 24
4.1 Open Source and Community Building Strategy 24
4.2 CyberNEMO Eclipse Research Labs 25
4.3 Open Source Licences 25
4.4 Open-Source Ecosystem 26
5 Conclusions 28
6 References 29

List of Figures

Figure 1: CyberNEMO Dissemination & Communication strategy 10
Figure 2: CyberNEMO Dissemination and communication strategy. Intensity increases each year 10
Figure 3: CyberNEMO X channel 12
Figure 4: CyberNEMO LinkedIn 13
Figure 5: CyberNEMO YouTube channel 13
Figure 6: CyberNEMO website (front page) 14
Figure 7: CyberNEMO website (news section) 15
Figure 8: Framework for successful, business-friendly open-source 25
Figure 9: The CyberNEMO project structure at ECLIPSE Labs. 25

List of Tables

Table 1: Preliminary list of events and conferences of interest to CyberNEMO. 16
Table 2: Identification of alliances and organizations where CyberNEMO Partners are active 22

List of Acronyms and Abbreviations

AIOTI	Alliance for Internet of Things Innovation
API	Application Programming Interface
BDVA	Big Data Value Association
CNCF	Cloud Native Computing Foundation
ENoLL	European Network of Living Labs
NGI	Next Generation Internet
SAI	Securing Artificial Intelligence (WG)
TC	Technical Committee
WG	Working Group
WP	Work Package
5GPPP	5G Public Private Partnership

Executive Summary

Deliverable D6.5 presents the initial status on the dissemination, standardisation and communities liaison plans for the CyberNEMO project. It contains the list of the current actions and time scales.
The outcomes resulting from the dissemination, standardisation, and communities liaison tasks will also be reported within the future releases of this deliverable.

1 Introduction

The objective of the work package "WP6 Impact Creation & Outreach" is to increase the visibility of the CyberNEMO project to attract the first users and to encourage the current consortium to continue and maintain the project. In other words, the objective of WP6 is to sustain the project by initiating a community of consumers and developers of CyberNEMO technologies.
In particular, the work package will form an Advisory Board for collecting feedback and advise on system approach. Further, the WP aims to consolidate project results and prepare the ground for their large-scale exploitation, also by triggering the scientific and technical communities to bring forward the state of the art on project technologies. Furthermore, the work package aim is to setup communication channels to disseminate the project outcomes as well as contribute to relevant Open-source communities & foundations, standards organizations and associations.
The document describes the initial dissemination plan, the list of ongoing and upcoming actions and timelines. Furthermore, Standardization activities and Community liaison will be taken into consideration with dedicated chapters.

1.1 Relation to other activities

This document is related to the Tasks 6.3, 6.4 and 6.5. The aim of these tasks is ensuring knowledge transfer and awareness of CyberNEMO solution in selected open-source communities and foundation, present the set-up of the communication channels and assets, including the website, the logo and the various social media accounts as well as present the initial standardization and communities liaison work.

1.2 Document overview

This document presents the initial plan and strategy of CyberNEMO about impact and outcome. In Section 2 the initial dissemination and communication actions are reported along with the social media dedicated channels. Section 3 presents the main standards, alliances and associations identified by the consortium for CyberNEMO and Section 4 presents the initial open-source strategy and actions. Section 5 concludes the document.

2 Dissemination & Communication Plan

The Dissemination and Communication plan describes how the project will create and follow effective dissemination and communication activities to promote CyberNEMO, the adoption of its outcomes also beyond project's lifetime and to engage its stakeholders.

The CyberNEMO dissemination and communication plan covers the following aspects:

- Objectives and goals of the envisioned activities (the what).
- Preliminary identification of stakeholders and target groups to be engaged (the whom).
- The methodology to be implemented to effectively engage these actors (the why).
- A plan of the specific activities that will evolve in line with the development of the overall project work and activities, in close collaboration with the rest of CyberNEMO Work Packages (the how).

The overall dissemination and communication strategy aims to creating synergies, contribute to partnerships development and knowledge sharing among stakeholders, while optimizing the resources and reducing the time between the news production and its delivery to the CyberNEMO wide audience, towards the following objectives:

- Trigger the scientific and technical communities to bring forward the state of the art on project technologies.
- Setup communication channels to disseminate the project's outcomes and build a Culture of Cybersecurity.
- Contribute to relevant Open-source communities & foundations, standards organizations and associations.
- Community liaison associated work with cybersecurity as a focus

2.1 Dissemination & Communication Strategy and Phases

The main goal of the CyberNEMO dissemination and communication activities is to raise awareness on the CyberNEMO technological and scientific achievements. An efficient impact of CyberNEMO must be supported by the development and implementation of a Dissemination strategy.
The relevant task coordinates the scientific dissemination and public outreach in tandem with the industry focus. CyberNEMO will be active at research and scientific events, as well as major exhibitions, while building a Culture of Cybersecurity. A detailed plan will be specified where a list of relevant research events (exhibitions, conferences, workshops, journals) to be pursued during the lifetime of the project will be kept. CyberNEMO academic partners will run training sessions for employees within their institutions, MSc, PhDs and MOOC, including graduate students. Finally, SYN created a website and UPM established the social channels to disseminate the project and update them regularly.
CyberNEMO success will be measured based on its market penetration and adoption by open-source communities, public authorities, CI, supply chain stakeholders and private companies, along with its impact on the "economic multipliers", that is SMEs. As such the main dissemination and communication activities' goal is to raise awareness on the CyberNEMO technological and scientific achievements. The Dissemination Plan will lay down the foundations for effective external communication, implementing the strategy shown in Figure 1, which focus on:

- Definition of the dissemination/communication strategy and target audience
- Fine tune the message, methodology, activities and material (e.g. press releases, research papers, white papers, videos, workshops, meetings, policy briefs, open days, promotional material) and the correct timing.
- Monitor and evaluate the public outreach activities, including redefinition and corrective actions.

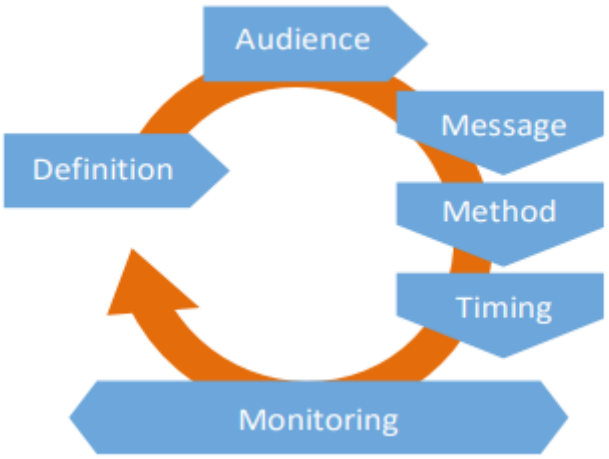


Figure 1: CyberNEMO Dissemination & Communication strategy

All the activities of dissemination and communication strategy will be carried out using three main phases, presented in Figure 2, following the different phases of the project. Each of these phases has specific objectives and target groups and will therefore perform specific actions using specific channels during the phase.

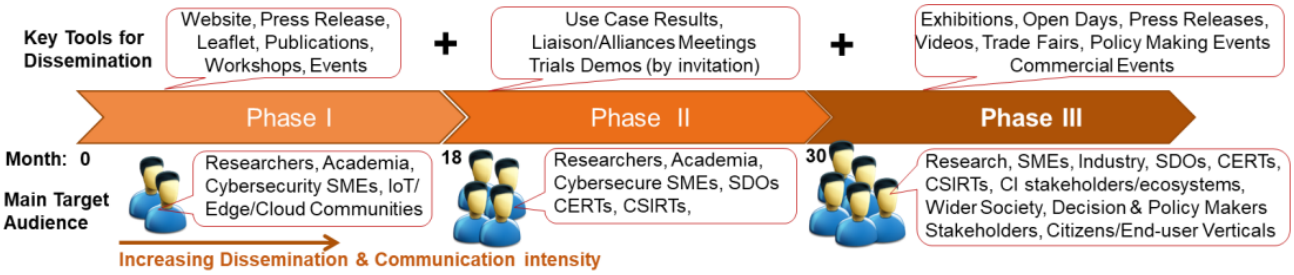


Figure 2: CyberNEMO Dissemination and communication strategy. Intensity increases each year

- Phase I (Months 1-18): Selecting and establishing the dissemination channels, key messages, communication activities towards innovation, IoT/Edge ecosystems/communities (Long time-to-market)
- Phase II (Months 19-30): Policy fostering business innovation (Midterm time-to-market).
- Phase III (Months 31-36): Matching market analysis and Exploitation (Short time-to-market).

2.2 CyberNEMO Dissemination and Communication

2.2.1 Stakeholder analysis

One of the CyberNEMO core objectives is the widespread awareness, adoption and impact creation of the outcomes achieved throughout the project. To become successful in such task, a specific plan is required to interact with key stakeholders, establishing, maintaining and growing a committed community around CyberNEMO.
The first stage of the strategy requires to understand which stakeholders CyberNEMO will engage with and for what purpose. Specific profiles that need to be identified to be involved or targeted. The objective is to facilitate a standard taxonomy of roles to be taken into consideration while assessing use case scenarios and new business models.
MetaOS is an evolving concept in next-generation operating systems that integrates cloud, edge computing, AI, and distributed systems to create a seamless and intelligent computing experience. It is designed to provide interoperability across devices, applications, and platforms, making it highly valuable for various stakeholders.

- Enterprises and business
- End Users & Consumers
- Cloud & Edge Service Providers
- Iot & Smart devices manufacturers

To maximize the stakeholders' interest and uptake, CyberNEMO will adopt the following best practices:

- Ensure open collaborative development, code review/management from the projects start, establishing CyberNEMO as an ECL project and hosted in well-established open-source Eclipse Research Labs (e.g. GitLab).
- Focus specifications on flexibility, adaptability open APIs and standardization, via adapters and plugins
- Align CyberNEMO roadmap and applications with industrial partners and end user's commercial strategies
- Adopt business friendly open-source licenses that enable collaborative open-source and business exploitation
- Build on existing Open-Source Communities, ecosystems and initiatives (i.e. AIOTI, DAIRO/BDVA, GAIAX, NGI, ENoLL, 5GPPP, CNCF, ROS) to establish liaisons and promote CyberNEMO
- Assign to ECL the role of supporting CyberNEMO maintenance and update after the end of the project
- Develop on-line documentation and guidelines for prospective contributors, policy makers and end-users

2.2.2 Social Media Dissemination

The social media channels will help create awareness about CyberNEMO project as well as giving a good approach to the day-to-day activities related to the consortium, such as participation in events, publication of papers and deliverables or the organization of workshops and general meetings.

Besides the social media channels created for the project, a newsletter will be delivered every 6 months as a summary of the activities done by the consortium within that period. Also, a Zenodo account to disseminate publications within the scientific community.

2.2.3 Online Channels

The project has foreseen the creation of CyberNEMO accounts in three social media networks; X, LinkedIn and YouTube. Here is the status of those SoMe channels at this point of the project.

- X: @HE_cybernemo



Figure 3: CyberNEMO X channel

- LinkedIn: www.linkedin.com/in/he-cybernemo-project

Due to the characteristics and outreach of LinkedIn, this social network is especially relevant to CyberNEMO project. For this reason, we will focus on it. At this moment of the project, we have 62 followers, and 59 contacts made. As for publications we have 5 posts shared with our community.



Figure 4: CyberNEMO LinkedIn

- YouTube: https://www.youtube.com/@CybernemoProject

The purpose of the creation of this video channel is to host the videos of the project, not only general but also the ones related to the pilots. but no video content yet, as we are waiting for the first results of the project to be released in the coming months.

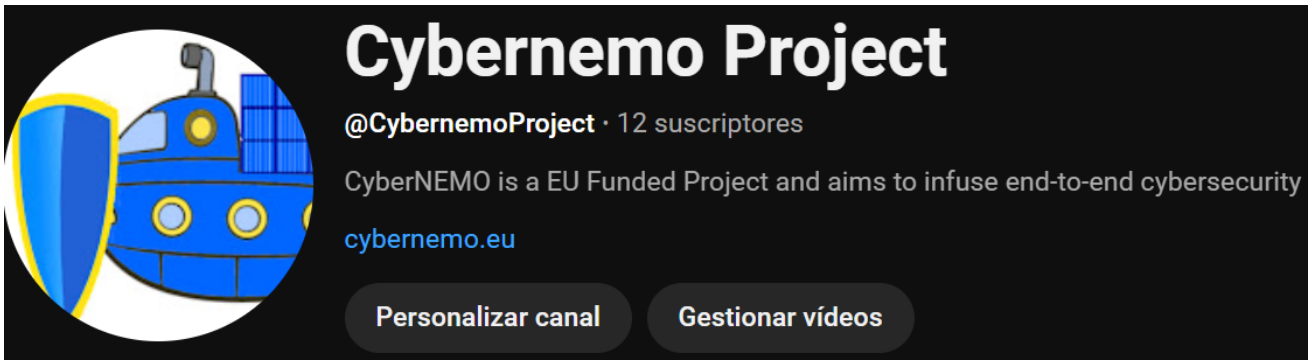


Figure 5: CyberNEMO YouTube channel

- The project website (URL: https://cybernemo.eu/)

The project website provides for the online presence of the project and offers useful information on the project, the public deliverables (when they become available) as well as information on the trials.

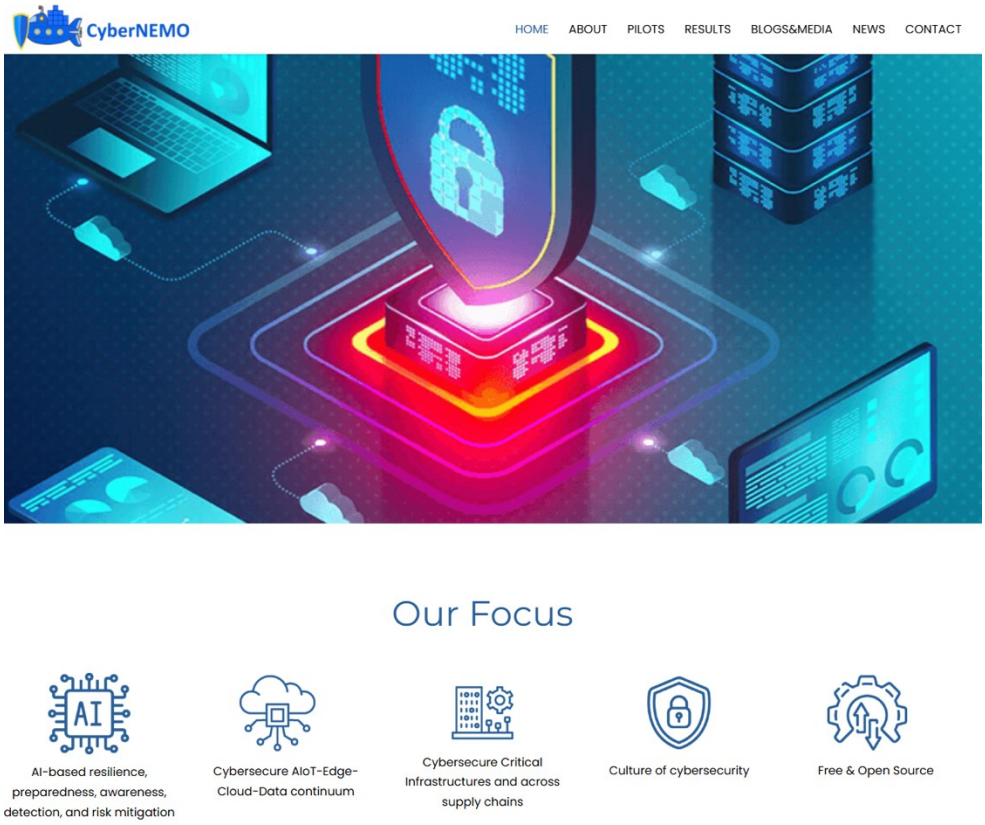


Figure 6: CyberNEMO website (front page)

Inside the website there are specifically two sections in which the activities of CyberNEMO are written. They are named “blog” and “news” sections, where several posts can be found published already, all related to the activities of CyberNEMO.
The website presents carefully curated information about CyberNEMO, structured to highlight the project's key elements in an accessible and comprehensible manner. It emphasizes interdisciplinary connections across technological fields, application domains, and research areas.
The website is designed to organize information effectively, enabling users to find content of interest with ease. Responsiveness across various client devices is prioritized, accommodating the diverse range of devices that may be used to access the site.
Activity on the website will be tracked in compliance with privacy and legal regulations, including adherence to the General Data Protection Regulation (GDPR) 2016/679.
Proper acknowledgment of the EC's financial support will be prominently displayed on the website.
The objectives and outlines of the website and social media channels are detailed in deliverable D6.1.

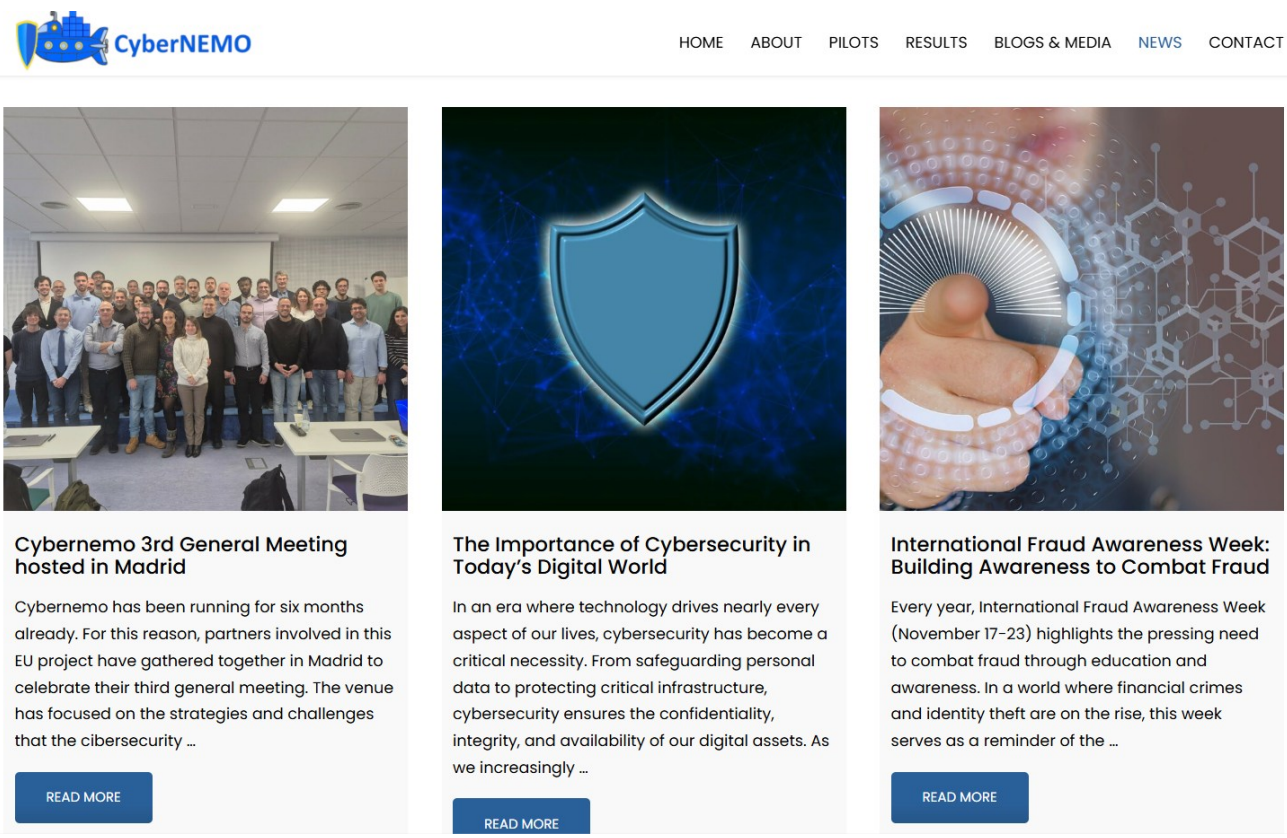


Figure 7: CyberNEMO website (news section)

As an indicative example of the blogs posted, the interested reader may refer to https://cybernemo.eu/index.php/2025/01/15/innovation-at-universidad-politecnica-de-madrid-the-role-of-gatv-in-cybersecurity/. In the news section, where the key activities of the project get advertised, a series of posts have been published, such as the following:

- https://cybernemo.eu/index.php/2024/11/11/international-fraud-awareness-week-building-awareness-to-combat-fraud/
- https://cybernemo.eu/index.php/2024/12/02/the-importance-of-cybersecurity-in-todays-digital-world/
- https://cybernemo.eu/index.php/2025/03/07/cybernemo-3rd-general-meeting-hosted-in-madrid/

To support the project's dissemination efforts, all partners have been encouraged to actively contribute to content creation by regularly sharing updates, insights, and materials related to their activities within the project. This includes drafting blog posts, providing technical summaries, sharing newsworthy developments, or contributing to social media content. A structured dissemination plan is in place to coordinate these efforts, with clear guidelines and timelines to ensure consistency and impact. A shared calendar and content tracker will help monitor contributions and identify upcoming opportunities for engagement, ensuring that all partners are aligned and that the project maintains a steady, engaging public presence.
For planning the content creation, we have created a CyberNEMO Blog Planning document. In the other hand for tracking and controlling the dissemination we have another relevant document.

2.2.4 Participation to events

This section will include a table that summarizes the events where the project has participated in the past. The table provides information about the event, including the date, and a brief description of the project's contribution. Currently in the period addressed we do not have any participation in events besides the two general meetings that have taken place.
During the following months we are planning to participate in several upcoming events such as SecSoft 2025. We are exploring our potential participation in other events and conferences, as tabulated in Table 1.

Table 1: Preliminary list of events and conferences of interest to CyberNEMO.

Event/Conference name	Date	Location
Nexus Forum 2025	May 8 – 10, 2025	Hong Kong
CCCGrid 2025	May 19 – 22, 2025	Tromso, Norway
International Cyber Expo 2025	Sep 30 – Oct 1, 2025	London, England
InfoSec World 2025	Oct 17 – 29, 2025	Lake Buena Vista, (FL), USA
DCAI - International Conference on Distributed Computing and Artificial Intelligence	Jun 25 – 27, 2025	Lille, France

3 European CI security policy & Standardization

3.1 Identification of main standards, alliances and associations for CyberNEMO

In the following, we will address the European and International standards, which we want to closely follow due to their special relevance for the CYBERNEMO project.

ENISA: Since 2004, ENISA supports the pan-European Cybersecurity Exercises, the development and evaluation of National Cybersecurity Strategies and the CSIRTs cooperation. It performs studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, and others. It assures the development and implementation of the European Union's policy on matters relating to network and information security and assists the European institutions in establishing and implementing vulnerability disclosure policies on a voluntary basis. Since 2019, it draws up cybersecurity certification schemes.

INTRA is a member at ENISA.

AIOTI: The AIOTI (Alliance for Internet of Things Innovation) is a partner for the European Commission on IoT policies and programs, helping to the deployment of IoT Innovation in Real Scale Experimentation in Europe. It is a member-driven organisation with equal rights for all members. The document published by the WG3 in October 2019 "IoT LSP Standard Framework Concepts" provides a list of IoT Standards Developing Organisation (SDO), Alliance and Open-Source Software (OSS) landscapes to be used as input for the recommendations for Large Scale Pilots (LSPs). In addition to the WG3 on IOT standardization, the topic of the WG11 is "Smart Manufacturing" and the topic of one horizontal WG is on Distributed Ledger Technologies. The Distributed Ledger Technologies WG is working on mapping current Blockchain implementations, rate the models toward current legal compliance (incl. GDPR), assist all existing AIOTI WG's on Blockchain implementations and develop Blockchain ecosystems across verticals.

SYN, RTWH and INTRA are participating in AIOTI.

ETSI: The European Telecommunication Institute works in different types of committees: TC (Technical Committees) addressing standardization activities in a specific technology area, Projects (EP) similar but established for a fixed period of time, ETSI Partnership Project established when there is a need to cooperate with other organizations to achieve a standardization goal and Industry Specification Group (ISG) focusing on a specific activity.

Several ETSI committees provide opportunities to demonstrate and validate proposed standards and to contribute project results to them. The TC SAI (securing artificial intelligence) WG focuses on securing artificial intelligence and provides trustworthiness for AI models and applications. The ISG ZSM (Zero Touch Network & Service Management) focuses on network automation and provides mechanisms and solutions to enable zero touch network. ETSI TC DATA (Data Solutions) focuses on standards for data interoperability, privacy, and responsible sharing across IoT and telecom sectors.

TID is chairing the ISG ZSM (Zero Touch Network & Service Management) and the recently created TC DATA (the Technical Committee on Data Solutions), and is active in TC CYBER (cybersecurity), TC SAI (Securing Artificial Intelligence) and ISG ENI (on AI application to network management). TSG is an active member of the TC SAI (Securing Artificial Intelligence).

IETF: The Internet Engineering Task Force develops Internet standards that are widely adopted by users, network operators, and devices. The IETF influences in the evolution of the Internet, but do not govern it, encouraging participation from anyone interested, promoting inclusivity and diversity while adhering to principles of open processes, technical expertise, and a volunteer-driven, consensus-based decision-making approach. The IETF publishes technical standards, encapsulated in Requests for Comments (RFCs), that outline Internet protocols like DNS or TLS. The process begins with an Internet-Draft created by participants in a working group, which, after rigorous review, is finalized into an RFC. The IRTF (Internet Research Task Force) is a parallel organization focusing on long-term research issues.

TID participates in the area of security, including the groups related to attestation (RATS), supply chain security (SCITT), Network management (NMRG) and SKEX (key management).

Eclipse Foundation for the community building with initiatives like ECLIPSE EdgeNative and IoT Working Groups to position CyberNEMO in the European Open Source IoT landscape.

ECSO: The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016. ECSO is the private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cybersecurity. It unites a variety of European cybersecurity stakeholders across the EU Member States, the European Free Trade Association (EFTA) and H2020 Programme associated countries. ECSO's main goal is to develop a competitive European cybersecurity ecosystem, to support the protection of the European Digital Single Market with trusted cybersecurity solutions, and to contribute to the advancement of the European digital autonomy.

TSG and ENG are participating in ECSO.

6G-IA refers to the 6G Smart Networks and Services Industry Association (6G-IA). It is the voice of European Industry and Research for next generation networks and services. Its primary objective is to contribute to Europe's leadership on 5G, 5G evolution and SNS/6G research. The 6G-IA represents the private side in both the 5G Public Private Partnership (5G-PPP) and the Smart Networks and Services Joint Undertaking (SNS JU). In the 5G-PPP and SNS JU, the European Commission represents the public side. The 6G-IA brings together a global industry community of telecoms & digital actors, such as operators, manufacturers, research institutes, universities, verticals, SMEs and ICT associations. The 6G-IA carries out a wide range of activities in strategic areas including standardization, frequency spectrum, R&D projects, technology skills, collaboration with key vertical industry sectors, notably for the development of trials, and international cooperation.

The 6G-IA Security working group aims to bring together the projects within the 6G SNS-IA that have a common interest in the development and progression of topics related to 6G security. The group will ensure, to as great an extent as possible, that the projects are working in a complimentary manner towards consistent goals, exchanging ideas, minimizing the duplication of effort, contributing towards relevant standards and where possible cooperating on the development of compatible components, demonstrators, the exchange of expertise, experience and results.

TSG is co-chairing the 6G-IA security working group, and UPM is an active participant in this WG. TID is the chair of the 6G-IA Spectrum WG and contributes actively to the Security WG, the Architecture WG and the Pre-standardization WG.

OASIS was founded under the name "SGML Open" in 1993 as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalized Markup Language (SGML). The consortium changed its name to "OASIS" (Organization for the Advancement of Structured Information Standards) in 1998 to reflect an expanded scope of technical work.

There are several active OASIS Technical Committees linked to C4IIoT innovations:

- "*Extensible Access Control Markup Language (XACML)*" which represents and evaluates access control policies.
- "*Message Queuing Telemetry Transport (MQTT)*" which provides a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.
- "*PKCS 11*" which enhances PKCS #11 standard for cryptographic tokens controlling authentication information (personal identity, cryptographic keys, certificates, digital signatures, biometric data)

TSG is participating in OASIS in different technical committees.

3GPP: The 3GPP covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provides a complete system description for mobile telecommunications. The 3GPP specifications also provide hooks for non-radio access to the core network, and for interworking with non-3GPP networks.

TID represents the Telefonica Group in 3GPP, with special focus on SA5 (management) and SA3 (security).

DAIRO: The association promotes Data, Big Data and Data-Driven AI research and innovation. Its main activities consist of:

- Developing strategic goals and roadmaps for research, development, innovation and deployment of European AI, Data and Robotic solutions, and supporting their implementation.
- Contributing to policy development, education and technology ramification in the widest possible sense, and addressing ethical, legal, and societal issues.
- Developing pre-standardisation activities and influencing standardization bodies.
- Supporting the federation of European experimentation AI, Data and Robotics infrastructures, digital innovation hubs and similar infrastructures.

In 2021, BDVA changed the legal name to DAIRO (Data, AI and Robotics AISBL). This new name testifies the ambition of the association to closely collaborate with other communities to jointly engage all the intersection of the key disciplines of Data, AI and Robotics.

ENG is a WG leader in DAIRO. UPM and INTRA are members in DAIRO WG Mobility & Logistics.

GAIA-X: GAIA-X is an initiative to develop a federated secure data infrastructure for Europe, whereby data are shared, with users retaining control over their data access and usage, and according to some to ensure European digital sovereignty. It aims to develop digital governance, based on European values of transparency, openness, data protection, and security, which can be applied to cloud technologies to obtain transparency and controllability across data and services.

UPM is participating in GAIA-X.

CEN: the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 34 European countries. CEN provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes. CEN supports standardization activities in relation to a wide range of fields and sectors including air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging.

CENELEC prepares voluntary standards in the electrotechnical field, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market.

CENELEC supports standardization activities in relation to a wide range of fields and sectors such as Electric vehicles, smart grid, smart metering, solar (photovoltaic) electricity systems, etc.

CEN-CENELEC Joint Technical Committee 21 on Artificial Intelligence created a dedicated task group (TG) dedicated to inclusiveness to help facilitate the participation of all relevant stakeholders in AI standardization. Multiple of the standards being developed in this task group is planned to become harmonized standard supporting the EU AI Act. This means being compliant to the standards e.g. for cyber security made in WG5, will presume compliance with the act, while engineering aspects are addressed in WG3, covering also data governance and quality. A similar effort of harmonized standards is in the making for Cyber Resilience Act. These standards are planned to become part of or harmonized with the legislations and standards to be used by EU notified body certification regimes for product certification, in short often called CE marking.

CSL and DNV are participating in CEN-CENELEC JTC21. Moreover, DNV is editor for the upcoming risk standard in this comity. CSL contributed to the CEN/CLC TR 18115:2024 “Data governance and quality for AI within the European context”.

NetworldEurope is the new incorporation of the European Technology Platform (ETP) for communications networks and services, the follow-up of Networld 2020 to follow the European changing policies as stated in Horizon Europe. Communications networks and services enable interaction between users of various types of equipment, either mobile or fixed, to fulfil society’s requirements for interconnection. They are the foundation of the Internet

and of our digital society. NetworldEurope ETP gathers players in the communications systems sector: industry leaders, innovative SMEs, and leading academic institutions, thus reaching out to a significant part of the European ICT community.

CSL is a member of Networld Europe. This network has reported the success story of the ReD component, that is the core of the PPE service in CyberNEMO.

OpenID: the OpenID Foundation (OIDF) is a global open standards body committed to helping people assert their identity wherever they choose. It was founded in 2007 and it is a global vibrant community where identity peers and thought leaders convene to craft the identity ecosystems of tomorrow. It is mission is to lead the global community in creating identity standards that are secure, interoperable and privacy-preserving.

TSG is an active member of OpenID.

NATO. Is a political and military alliance of countries from Europe and North America. Its members are committed to protecting each other from any threat. The NATO standardization agreement (STANAG) was created to build a common framework for security policies and confidentiality metadata to facilitate information sharing between member nations and industry partners. However, implementing the NATO STANAG 4774 and 4778 policies for classification can be complicated due to the disparate systems in use by member nations, nation-specific security classifications, and clearance levels.

A STANAG specifies the agreement of member countries to implement a standard. They provide a framework for interoperability, including common operational and administrative procedures and logistics, information systems (CIS), and formats to facilitate sharing of intelligence and other information for NATO and Allied operations.

STANAG 4774 outlines the metadata syntax required for a confidentiality label to better facilitate and protect sensitive information sharing. In addition, STANAG 4778 defines how a confidentiality label is bound to the data throughout its lifecycle and between the sharing parties. It also outlines cryptographic techniques to ensure the integrity of data and labels.

TSG is an active member of NATO STANAG 4774/4778.

CNCF. The Cloud Native Computing Foundation (CNCF) is a Linux Foundation project that was started in 2015 to help advance container technology and align the tech industry around its evolution.

It was announced alongside Kubernetes 1.0, an open-source container cluster manager, which was contributed to the Linux Foundation by Google as a seed technology. Founding members include Google, CoreOS, Red Had, Twitter, Huawei, Intel, Cisco, IBM, Docker, Univa, Mesosphre, and VMware. Today, CNCF is supported by over 450 members. In order to establish qualified representatives of the technologies governed by the CNCF, a program was announced at the inaugural Cloud native Day in Toronto in August 2016.

CNCF technology projects are catalogued with a maturity level of Sandbox, Incubated, and Graduated, in ascending order. The defined criteria include rate of adoption, longevity and whether the open-source project can be relied upon to build a production-grade product.

CNCF's process brings projects in as incubated projects and then aims to move them through to graduation, which implies a level of process and technology maturity. A graduated project reflects overall maturity; these projects have reached a tipping point in terms of diversity of contribution, community scale/growth, and adoption.

The CNCF Sandbox is a place for early-stage projects, and it was first announced in March 2019. The Sandbox replaces what had originally been called the "inception project level".

TSG is an active member of CNFC. TID participates in CNCF and is one of the main contributors to the related Sylva initiative.

ISO/IEC JTC1 is a Jointed technical committee of ISO and IEC created to promote standards in the fields of Information Technology and Information and Communication Technology. The interesting subgroups related to AI,

IoT are WG3 on IoT architecture, and AI trustworthiness, AI sustainability, WG4 on IoT interoperability and WG5 on IoT applications.

ISO/IEC JTC1/SC42 focuses on the standardization around Artificial Intelligence. It serves as the focus and proponent for JTC 1's standardization program on Artificial Intelligence. It also provides guidance to JTC1, IEC, and ISO committees developing Artificial Intelligence applications. The ISO/IEC JTC1/SC42 WG3 focuses on AI trustworthiness. The ISO/IEC JTC1/SC 42/JAG is the Joint Advisory Group on AI and sustainability.

DNV is an active member of the ISO/IEC/JTC1/SC42 WG3 Trustworthiness, and CSL is an active member of the ISO/IEC/JTC1/SC42 and of the ISO/IEC JTC 1/SC 42/JAG.

3.2 CyberNEMO in European CI security policy

CyberNEMO aims to generate tangible blueprints for CI and supply chain risks and contribute to the implementation of the EU Security Union Strategy and an interconnected cross-CI security roadmap. To achieve the goal, CyberNEMO will promote new work items in Standards Development Organisations (SDOs) relevant to cyber-physical security. CyberNEMO will significantly contribute to *ECSO* (European Cyber Security Organisation) activities, where ENG and TSG is active member and *EOS* (European Organization for Security), where ENG is founding members and members of the board of directors. Moreover, via *PSCE* (Public Safety Communication Europe Forum), CyberNEMO will share knowledge and expertise, leading to better protection of critical infrastructures against all types of threats and hazards. CyberNEMO partners INTRA will actively contribute to the ENISA coordinated *Stakeholder Cybersecurity Certification Group (SCCG)*. CyberNEMO Standardization. TSG and UPM are co-chairing the security working group in 6G-AI where the main focus is on applying AI for cloud native applications and 6G applications in terms of automation, detection, or remediation. TSG has an active participation in the CNCF community and will work to share the main goals of the project in relation with cloud native communications, and cloud continuum.

Synelixis participates in the *Alliance for AI, IoT and Edge Continuum Innovation* (https://aioti.eu/) and contributes to the convergence of AI, IoT and Edge Computing research and innovation, standardisation, and ecosystem building.

DNV and CSL through their presence in the CEN-CENELC JC21 and ISO/IEC JTC1 will be able to share their expertise and outcomes of the CyberNEMO project and therefore contribute to the working groups related to artificial intelligence and its trustworthiness.

CSL defines policy options regarding the ethics and regulatory challenges in the context of AI and cybersecurity and debates these options with policy makers and other relevant stakeholders.

UPM is participating in GAIA-X in order to develop a federated secure data infrastructure. It will be able to promote the results of the CyberNEMO project to the GAIA-X.

SYN, RWTH and INTRA are participating in the AIOTI alliance, where they will share knowledge about the deployment of IoT innovation in real scale experimentation.

In the following Table 1, we have identified the main alliances, organisations, and associations where CyberNEMO partners have strong presence. At this stage, we have identified also the possible contributions and the research axis where partners could contribute to these organisations.

Table 2: Identification of alliances and organizations where CyberNEMO Partners are active

Alliances/Organisations / Asso-ciations	Working Group	Partner	Position	Relation to CyberNEMO/Potential Contribution
CEN/CENELEC	CEN/CLC JTC21/WG3	CSL	Member	Trustworthy AI
CEN/CENELEC	CEN/CLC JTC21/WG5	DNV	Member	Joint standardization on Cybersecurity for AI systems. planned to become harmonised standard supporting the EU AI act
Networld Europe	SME WG	CSL	Member	Contribute to the convergence of 6G, AI, and IoT
AIOTI	Agriculture and Energy WG	SYN, INTRA	Member	AI, IoT and Edge Continuum ecosystem
AIOTI	Research, Standardisation, Policy, Smart energy	RWTH	Member	IoT and Edge Continuum ecosystem
ENISA	Stakeholder Cybersecurity Standardisation	INTRA	Member	Cybersecurity, SAAM alignment with MeliCERTes
DAIRO	WG Mobility & Logistics	INTRA, UPM, ENG	ENG (WG Lead); UPM (Member), INTRA (Member)	cybersecure homomorphic encrypted FML topics
6G-IA	Security Working Group	TSG, UPM	TSG (co-chair), UPM (Member)	AI based Security (monitoring, penetration testing), Computing Continuum.
ETSI	TC SAI (Securing Artificial Intelligence)	TSG, TID	Member	Securing AI, trustworthy AI, FML topics
ETSI	TC DATA (Data solutions)	TID	Convenor	standards for data interoperability, privacy, and responsible sharing across IoT and telecom sectors.
ETSI	ISG ZSM (Zero Touch Network & Service Management	TID	Chair	Network automation for security and PoC
OpenID	AuthZen WG	TSG	Member	define standard mechanisms, protocols and formats for communication between authorization components, and recommend best practices for developing secure applications.
NATO	STANAGs 4774/4778/5663/5664	TSG	Member	Sensitive Information Sharing between multiple parties
CNCF	WG Open Source	TSG	Member	open-source communities, cloud native
Linux Foundation	WG Open Source	TSG	Member and Advisory Board	Open-source communities, raise awareness

Linux Foundation	Linux Foundation Energy	RWTH	Board and technical advisory council	Open-source communities
IETF	RATS (Remote ATtestation procedureS), supply chain security (SCITT), Network management (NMRG) and SKEX (key management).	TID	Member	Notary Service, trust path attestation, MnCC, CCIPS
ECSO	Policy Analysis and Outreach Stream	ENG	Member	close collaboration with EU policymakers and the integration of insights from both public and private sectors
ECSO	CTI Initiative	ENG	Member	public / private cooperation in the CTI domain
ISO/IEC JTC1 SC42/	WG3 Trustworthiness	DNV	Member	AI trustworthiness
GAIA-X	GAIA-X Spanish Hub	UPM	Member	Federated and secure Data infrastructure
Eclipse Foundation	Eclipse Foundation	ECL	ECL is a member of the project	IoT ecosystem

4 Open Source Ecosystem and Community Building

4.1 Open Source and Community Building Strategy

The purpose of this activity will be to implement the open-source strategy to maximise up-take and achieve sustainability of project results beyond the project lifetime.
The strategy will work on several aspects, create and integrate CyberNEMO in a rich online community, draw with CyberNEMO the plan to contribute to existing communities and open-source projects like NEMO. It will lay out the plan and means to contribute to relevant existing open-source projects and communities and define licensing guidelines (inbound and outbound).
One of the key points in the strategy is sustainability and the focus will be to integrate CyberNEMO in a community. In particular, one of our priorities will be the creation of a rich online community, which includes end users that participate in the internal use cases (WP6), innovators, and all types of stakeholders interested in fostering the uptake of CyberNEMO outcomes. This will support the creation of an active community of developers and early adopters.
In summary, the key aspects of a good open-source strategy are:

- to draw and keep track of the open-source landscape of the project,
- to create an environment that allows doing proper open-source, and
- to lay out measures for community building, sustainability and long-term governance.

These aspects materialise in the following concrete actions for implementing the CyberNEMO open-source strategy:

1. Identify what partners bring into the project. As an initial step of the landscaping activities, all the assets that partners bring into the project will be identified. This effort has been started during the proposal phase and is currently being refined with a more in-depth analysis with all technical partners.
2. Identify open-source outputs. The second part of the open-source landscaping activities is related to the project outputs: Will the project develop new tools or products? Does it aim to provide a full-fledged integrated platform? Does it aim to extend or contribute significantly to already existing tools that partners bring into the project? Or probably a combination of all of those? It's important to identify and state as clearly as possible which parts of the project results will be open-source and of what nature they will be, answering to the above questions. This activity contributes to a coherent open-source landscape of the whole project. It has started and is currently work in progress.
3. Target relevant open-source communities. When an initial open-source landscape is drawn, relevant communities can be identified. Naturally, these communities are to some degree defined by open-source projects that partners bring into the project but it is always worth thinking about other communities beyond the obvious ones. When the initial steps have been made and the project has reached a solid architecture and definition, a close work with the dissemination activities will start also by considering ambassadors and influencers could be hired to disseminate the project in their ecosystems (e.g., technology leaders from Eclipse IoT & Edge Working Groups). In parallel, the content strategy for the community will be defined while a digital campaign will be organised to widely advertise the community within relevant domains in the EU. Content related activities such as posts, events and interactive activities, such as Q&A, webinars, will be continuously organised to keep users engaged with the community and success stories and/or Testimonials interviews will be drafted. Close collaboration with standardisation, dissemination, and exploitation. Take care of IP and licensing. Discussing open-source licences is important. The consortium should agree on (the types of) licences for the project results, based on the open-source licensing processes defined in the CA. For example, to allow for commercial exploitation of the open-source results, strong copyleft licences should not be allowed to be brought into the project (at least not without prior agreement). When the project is running and code is being developed, it will be wise to keep track of all the inbound IP and licences. The goal here is to identify issues as early as possible. e.g. exchanging a GPL'ed library will be much easier when detected early, than it will be later, when a lot of code is already depending on it. The CyebrNEMO open-source strategy is based on business-friendly open-source to allow for exploitation of the results. Training, coordination and support on open-source licensing will be provided throughout the project.
4. Develop in the open early. As the name indicates, open-source development is meant to happen in the open. In most cases it is not a good idea to wait until the end of the project because "the code has to be polished before showing it to the public" or "is not ready yet" for whatever reason. Developing behind closed walls is an open-source antipattern. It will slow down the project and the effort to "do it later" will keep growing. Therefore, efforts to set up the project's infrastructure (i.e. a public repo) and training

on open-source best practices are underway. The goal is to implement these best practices at the heart of CyebrNEMO to foster knowledge transfer and unleash all the benefits of open collaboration.

4.2 CyberNEMO Eclipse Research Labs

CyberNEMO open-source strategy is well integrated with the Eclipse Foundation framework for successful, vendor-neutral, business-friendly open-source. This framework (see Figure 1) is based on four main pillars: (i) infrastructure for open collaboration & development (ii) integration relevant open-source communities and business ecosystems (iii) governance for managing successful open-source projects and community building and (iv) intellectual property (IP) management that ensures IP is tracked and properly managed and open-source project results can be exploited by academic and commercial partners alike. This framework is operationalised by the CyberNEMO open-source strategy.

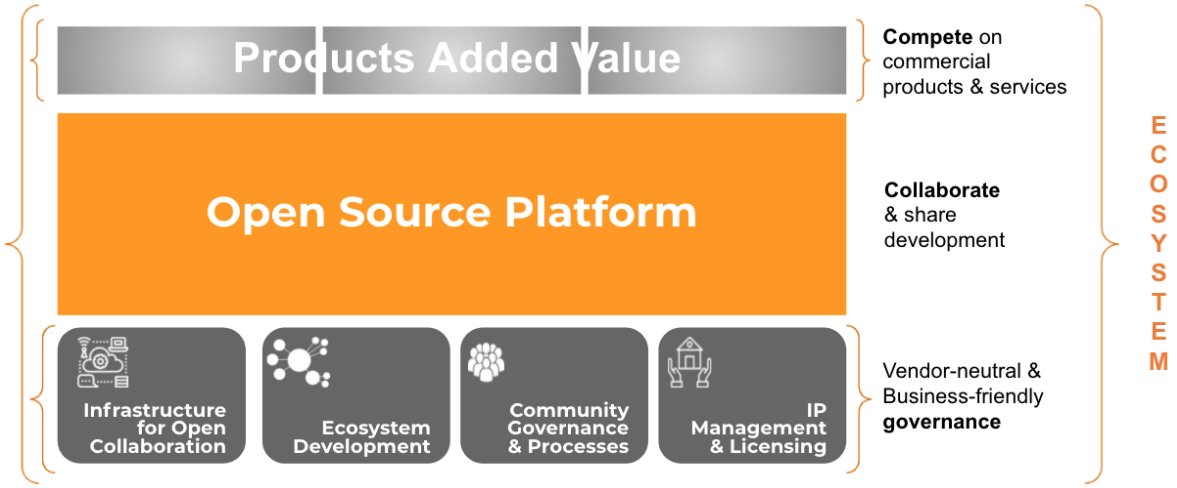


Figure 8: Framework for successful, business-friendly open-source

In order to achieve this vision and starting an open-source development practice, Eclipse provide an open-source repository called CyberNEMO Research Labs

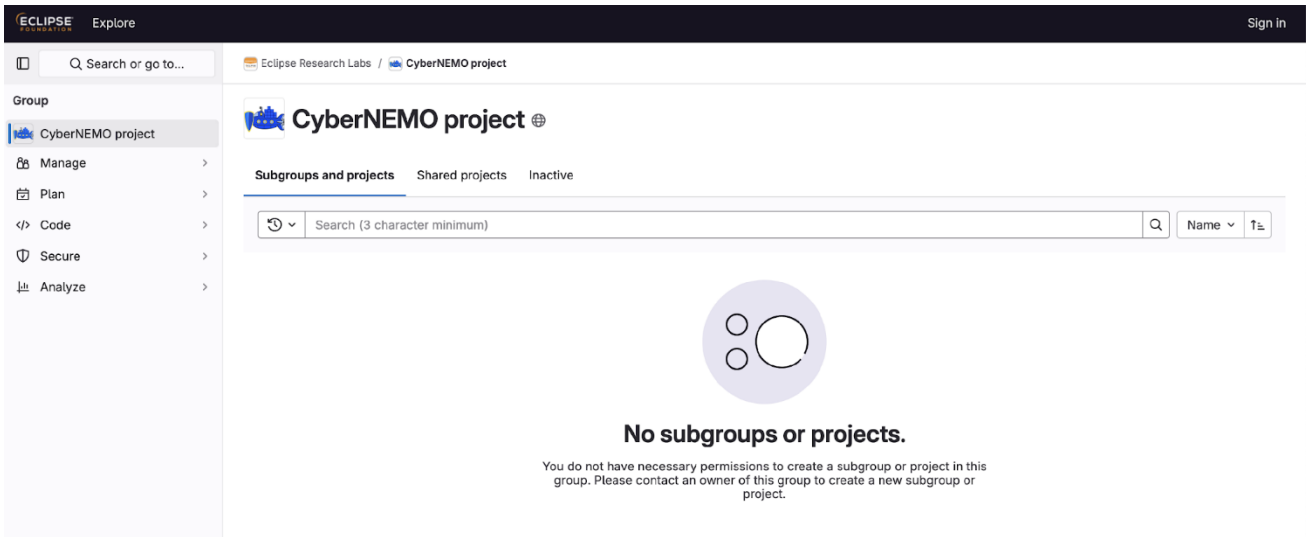


Figure 9: The CyberNEMO project structure at ECLIPSE Labs.

4.3 Open Source Licences

Open-source licenses are legal frameworks that define how software can be used, modified, and distributed. CyberNEMO will consider an open-source license. In this document, a high-level overview of the main types discussed so far is presented:

- Permissive Licenses:
  - Allow users to freely use, modify, and distribute software with minimal restrictions
  - Examples: MIT License, Apache 2.0, BSD 3-Clause.

Key Feature: No requirement to release source code when distributing modified versions (though the original must still credit the author).

- Copyleft Licenses:
  - Require that any modified versions of the software be distributed under the same license, ensuring it remains open-source.
  - Examples: GNU General Public License (GPL)

Key Feature: Ensures modifications remain open-source and that improvements are shared with the community.

- Weak Copyleft Licenses:
  - Similar to copyleft, but less strict. Only certain components (like the modified code) must be open-source, not the entire project.
  - Examples: Eclipse Public License (EPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL).

Key Feature: Allows combining open-source with proprietary code in certain cases.

- Permissive Licenses:
  - "Permissive" or "Non-Copyleft" Free software comes from the author with permission to redistribute and modify, and add additional restrictions to the license terms.
  - Examples: APACHE, BDS, MIT.

Key Feature: Allows modifying the non-copyleft program and distributing the modified program as a proprietary software product, without making the source code available to others on the same terms.

Each open-source license is designed to balance between providing freedom to users and protecting the interests of the original authors. The choice of license depends on how the author wants the software to be used and shared.

4.4 Open-Source Ecosystem

CyberNEMO will exploit the open-source ecosystem of one of the world's largest open-source software foundations, in fact the Eclipse Foundation plays a crucial role in fostering an open, collaborative, and business-friendly open-source ecosystem. Its projects and working groups span multiple industries, enabling innovation while ensuring strong governance, IP management, and security.
The Eclipse Foundation hosts over 400 open-source projects across various domains. Some key projects include:

- Eclipse IDE – A popular open-source integrated development environment.
- Jakarta EE – The evolution of Java EE for enterprise applications.
- Eclipse Che – A cloud-based developer workspace.
- Eclipse Theia – A flexible, web-based IDE alternative to VS Code.
- Eclipse IoT – A set of frameworks and tools for building IoT solutions.
- Eclipse MicroProfile – A set of Java-based microservices specifications.
- Eclipse SUMO – A traffic simulation tool widely used in smart mobility research.

The Eclipse Foundation collaborates with various industries, providing specialized working groups, including:

- Adoptium (formerly AdoptOpenJDK) – Builds OpenJDK binaries.
- Eclipse IoT – Focused on IoT standards and interoperability.
- Eclipse Automotive (SDV) – Supports software-defined vehicle initiatives.
- Eclipse OSGi – A dynamic module system for Java.

- Eclipse Edge Native – Focused on edge computing solutions.

Furthermore, Eclipse works closely with standardization bodies in order to support industry-wide open standards.

5 Conclusions

In this document the initial plan and strategy of CyberNEMO about dissemination, communication, European CI security policy and standardization, and open-source ecosystem and community building have been presented.
The initial dissemination and communication actions are reported along with the social media dedicated channels and the social media dissemination the strategy and phases.
The document also presents the main standards, alliances and associations identified by the consortium for CyberNEMO and the European CI security policy related to the standards.
Finally, CyberNEMO will implement an open-source strategy, fostering active engagement with developer communities and early adopters. Working closely with CyberNEMO consortium innovators, the task focuses on identifying relevant open-source assets, developing a community-building strategy, and establishing good open-source practices. With this aim, the Eclipse framework includes professional governance, IP/license management, and active participation in events, creation of communication materials, and organization of workshops to promote CyberNEMO within the developer communities.

6 References

[1] CYBERNEMO, "D7.1 Project Handbook," Horizon Europe - CYBERNEMO - 101168182 - Deliverable Report, 2024.