



CyberNEMO

End-to-end Cybersecurity to NEMO Meta-OS

CYBERNEMO

Securing the MetaOS

Prousalidis Konstantinos, SYNELIXIS

26th InfoCom World Conference | 12 November 2024



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



Outline

- Project Identity Card
- Our Consortium
- Motivation & Vision
- CyberNEMO Digital Agenda
- Innovations & Impacts
- Validation



Project Identity Card

- **Title:** End-to-end Cybersecurity to NEMO Meta-OS
- **Grant agreement ID:** 101168182
- **HE Call:** HORIZON-CL3-2023-CS-01
- **Topic:** HORIZON-CL3-2023-CS-01-01
- **Funding Instrument:** IA
- **Coordinator:** SYNELIXIS (Project Coordinator)
- TELEFONICA (Technical Coordinator)
- **Duration:** 36 months – **Starting Date:** 1st October 2024
- **EU Contribution:** ~6 MEuros
- **Consortium:** 23 Partners
- **EU coverage:** 11 Countries
- **Validation:** 8 Use Cases – 4+1 Living Labs/Pilots



CyberNEMO
End-to-end Cybersecurity
to NEMO Meta-OS



Our Consortium



	Participant organisation name	Short name	Country	
01	Synelixis Solutions S.A. (SME)	SYN	Greece	Large Industry/ SMEs
02	DNV A.S.	DNV	Norway	
03	Thales Six GTS France S.A.S.	TSG	France	
04	Engineering – Ingegneria Informatica SPA	ENG	Italy	
05	Netcompany – Intrasoft S.A.	INTRA	Luxembourg	
06	SIEMENS SRL	SIEM	Romania	
07	Maggioli Group SPA	MAG	Italy	
08	Space Hellas S.A.	SPACE	Greece	
09	Cyber Ethics Lab (SME)	CEL	Italy	
10	Digital Systems 4.0 (SME)	DS4	Greece	
11	Unparallel Innovation LDA (SME)	UNP	Portugal	
12	Telefonica Digital Espana SLU	TID	Spain	Telecom Operator
13	Hellenic Telecom Organization S.A. (Deutsche Telecom Group)	OTE	Greece	Pilots/ Living Labs
14	ASM Terni SpA (Smart Energy, RES, Water/Wastewater Pilot)	ASM	Italy	
15	Entersoft S.A. (Logistics/Supply Chain Pilot)	ESOFT	Greece	
16	Medical University - Plovdiv Hospital (Healthcare Pilot)	MUP	Bulgaria	
17	Sorbonne Université	SU	France	Research
18	Universidad Politécnica De Madrid	UPM	Spain	
19	Rheinisch-Westfälische Technische Hochschule Aachen	RWTH	Germany	
20	University of Patras	UPAT	Greece	
21	Charles III University of Madrid	UC3M	Spain	
22	Eclipse Foundation Europe GmbH	ECL	Germany	Open Source Ecosystem
-	Sphynx Technology Solutions AG (SME)	STS	Switzerland	Associated Partner

Motivation & Vision





Motivation

- Transition from IoT to AIoT (Artificial Intelligence of Things)
 - “Connected things”, ranging from low-end devices, such as simple sensors and actuators to collaborating swarms of intelligent systems, such as autonomous cars, Unmanned Aerial Vehicles (UAV) and robots **need sufficient, real-time, secure and trusted support from the edge cloud**, including *storage, computational and processing resources*, along with *AI support*

while:

- Rising cybersecurity threats (increasing cyberattacks - zero-day)
 - Cybersecure and trusted Computing Continuum of IoT/Edge/Cloud/Data is required
 - with **less data** stored and processed **in central data centres**, and **more data processed closer to the user**, cybersecurity, privacy and security breaches will no longer be able to focus on protecting central points of connection (POC), but **consider any segment as non-trusted**



CyberNEMO vision

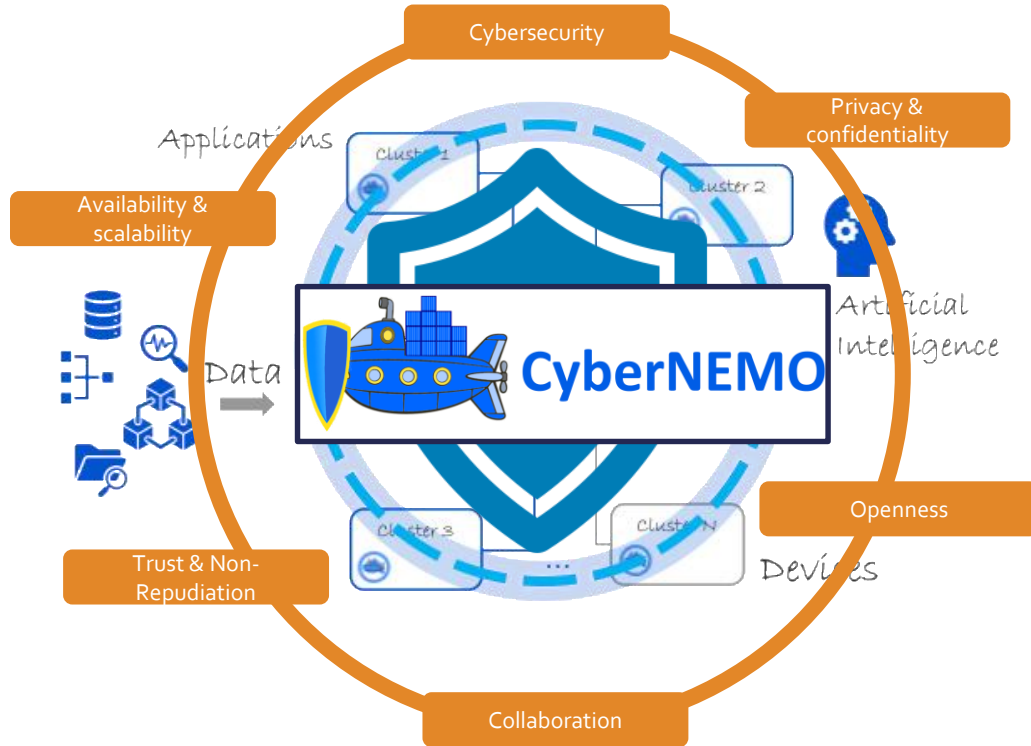
CyberNEMO will establish itself as a paradigm-shift towards
cybersecure AIoT-Edge-Cloud-Data continuum
by introducing an open source framework
to support Computing Continuum resilience, preparedness,
awareness, detection, and risk mitigation
within *Critical Infrastructures deployments and across supply
chains.*

CyberNEMO Digital Agenda





from NEMO to CyberNEMO



1. End-to-end CC cybersecurity, resilience, trust, privacy and policy enforcement
2. On-device AI to enable cybersecurity of self-aware, (semi-) autonomous entities
3. Internet-native Zero Trust Network Access (ZTNA)
4. AI-based data sovereignty protection, edge/cloud vulnerabilities detection/mitigation and privacy/data breaches protection
5. Preparedness, incidents' response, AI-based collaborative countermeasures
6. Vulnerability assessment cross-CI, supply chains and domains
7. Culture of cybersecurity

Innovations & Impacts

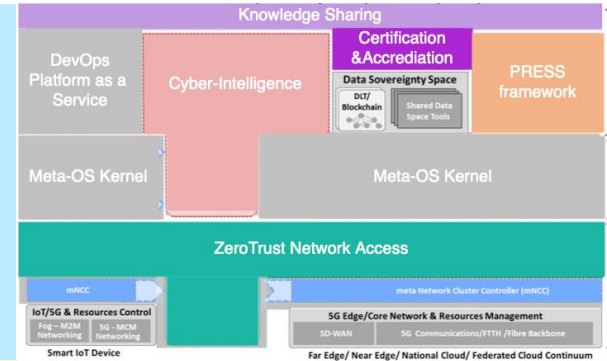




CyberNEMO innovations & impacts

Technological innovations

- End-to-end Cybersecure NEMO Meta OS
 - Cybersecurity and zero-trust into NEMO federated meta Network Cluster Controller (mNCC) to interface on demand existing/emerging IoT/5G/6G network management and routing protocols
 - Federated “by-design” and “by-innovation” extended Secure Access Service Edge (SASE) to support secure integration of untrusted IoT and secure micro-services intent based migration in trusted ecosystem.
- Intelligence closer to data & secure distributed learning via Zero Trust Federated ML
- Trusted collaborative cross-domain/cross-border Knowledge Sharing and Mitigation
- PRESS (Privacy, data pProtection, Ethics, Security & Societal) framework and GDPR compliance
- Certification & Accreditation



Creating sustainable impact for the EU

- Open and community building
 - open source, open APIs, open standards compliant
 - hosted and promoted as ECLIPSE project
- Standards compliant, following AIOTI, DAIRO/BDVA, GAIA- X
- Respecting EU values
 - data sovereignty, interoperability, GDPR and EU regulations

Expected (Technical, Economical, Environmental, Social) Impact

- Full-stack cybersecurity
- Business innovations in the ECI security sector
- Safeguarding European competitive position in cybersecure and dynamic data-agile economy
- New Digital services and revenue streams in Living Lab verticals
- CO2 reduction: AI-based energy aware workload scheduling/migration across edge and cloud resources; Smart Farming: streamlined and eco-friendly production processes
- Increased security for citizens and higher safety for users
- Creating new business/jobs in supply chain security

Validation





CyberNEMO Trials



Trial #1: CyberNEMO Integration Infrastructure Technology Lab



Trial#2: Smart Energy & Smart Water Critical Infrastructures



Trial #3: Secure and Intelligent Media Content Supply Chain Ecosystems



Trial #4: Proactive & Intelligent Protection of Healthcare Critical Infrastructures



Trial #5: Smart Farming and FinTech/Logistics Supply Chain



Trial #6: Pan-European SAAM multi-Living Labs Federation

Thank you for your attention

Konstantinos Prousalidis, SYNELIXIS



CyberNEMO

SYNELIXIS

Telefónica

DNV

THALES

OTE

SPACE

netcompany

intrasoft

SIEMENS

eng

Maggioli

ENTERSOFT

ASM
ASM Termi S.p.A.

UNPARALLEL

DigiSys 4eU

Sphynx
Technology
Solutions



CyberEthicsLab.

SORBONNE
UNIVERSITÉ



RWTHAACHEN
UNIVERSITY



POLITÉCNICA



ECLIPSE
FOUNDATION