This research project has received funding from the European Community's H2020 Programme, under grant agreement Nr. 830927. Funding scheme: H2020-SU-ICT-2018-2

# Cyber security cOmpeteNce fOr Research anD Innovation - CONCORDIA

National Cyber Security Authority of Greece

Ministry of Digital Policy, Telecommunications and Media

General Secretariat of Digital Policy

Contact: ncsa@gsdp.gr

## Introduction

CONCORDIA (2019-2022 H2020 project) positions the CONCORDIA ecosystem, a Cybersecurity Competence Network with leading research, technology, industrial and public competences to build the European Secure, Resilient and Trusted Ecosystem, with the CODE research institute in Munich to act as the coordinating center.

CONCORDIA will strongly liaise with ENISA to leverage its expertise and knowledge with ENISA being the interface to other cybersecurity actors and networks within the EU institutional framework and with established industry networks in the private sector, and playing the role of a secretariat (in a similar fashion to the way it offers secretariat functions to the CSIRT Network). Munich, as decided by the EC to be Europes top technology hub, gives the perfect ICT environment for CODE to be central hub of the network.

## Objectives

1. A Cybersecurity Competence Network with CODE research center as coordinator and ENISA as secretary
2. Using an open, agile and adaptive governance model and processes that combines the agility of a start-up with the sustainability of a large center
3. Devise a cybersecurity roadmap to identify powerful research paradigms, to do hands-on experimental validation, prototype and solution development .
4. Develop next-generation cybersecurity solutions by taking a holistic end-to-end data-driven approach
5. Scale up existing research and innovation with CONCORDIAs virtual lab and services.
6. Identify marketable solutions and grow pioneering techniques towards fully developing their transformative potential.
7. Develop sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators.
8. Launch Open Calls to allow entrepreneurs and individuals to stress their solutions with the development.
9. Set up an Advisory Board, comprised by leaders of industry, standardization, policy and politics.
10. Mediate between multiple communities
11. Establish an European Education Ecosystem for Cybersecurity
12. Provide expertise to European policy makers and industry


Figure 1. Goals of CONCORDIA.

## NCSA - National Cyber Security Authority

As Critical National Infrastructures are becoming more vulnerable to cyber attacks, their protection becomes a significant issue for any organization as well as a nation Moreover the synergy between the ICS and the IoT has emerged bringing new security challenges [1]. Modern smart societies face new challenges in the area of cyber security, and EU is struggling to strengthen Critical Infrastructures by publishing new directives [2].

Along with the obligations that directly arise out of the European directives and regulations, Greece and all other member states should also take further actions for enhancing cyber security. NCSA [3] is responsible for coordinating all competent Ministries and independent authorities of Greece, in order to take all necessary steps towards a secure Greek Cyber space. Its main objective is to Shield the Nation from external threats and to provide a secure digital environment for all citizens of Greece. NCSA has issued in 2018 both the National Cyber Security Strategy [4] and the National Law on security of network and information systems [5].

## Methodology

The unique selling point of CONCORDIA is its approach to innovation, openness, integration, agility, and also size. With more than 40 partners in CONCORDIA, especially more than 20 industry partners, this strong backbone of collaboration becomes obvious.

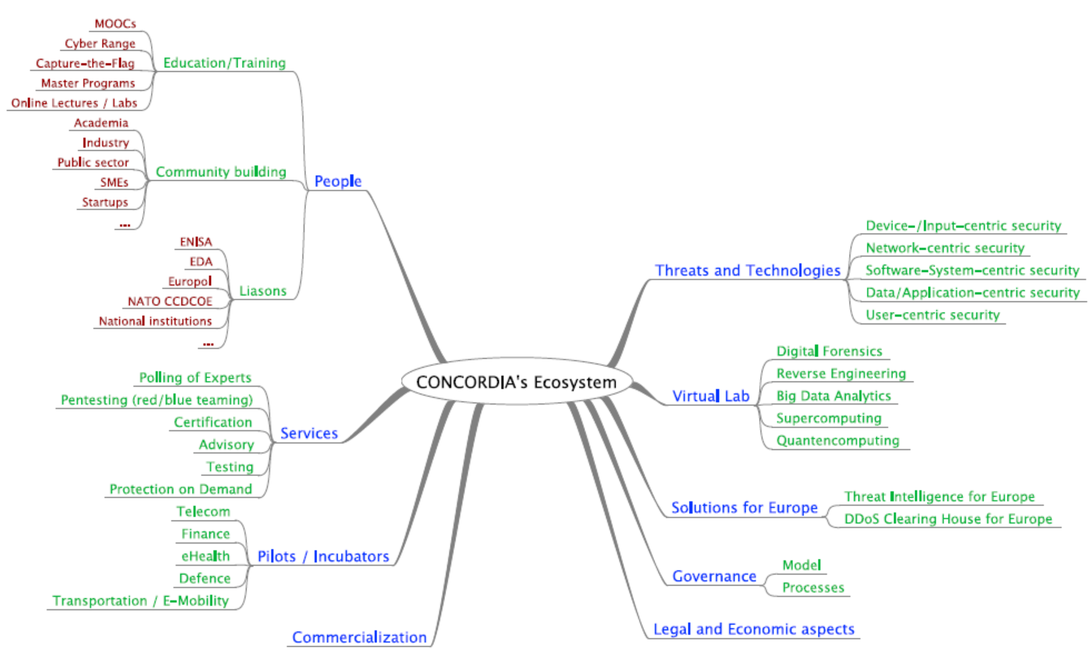


Figure 2. Overview of CONCORDIAs methodology dimensions.

CONCORDIA employs an overall methodology that spans the dimensions shown in Fig. 2 to ensure a scalable, successful, and long-lasting implementation.

## References

[1] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz, Cyber Security of Critical Infrastructures, ICT Express (Elsevier), Volume 4, Issue 1, March 2018, Pages 42-45, DOI: 10.1016/j.icte.2018.02.001

[2] Leandros A. Maglaras, George Drivas, Kleanthis Noou, Stylianos Rallis, "NIS directive: The case of Greece", EAI Transactions on Security and Safety, May 2018, DOI: 10.4108/eai.15-5-2018.154769

[3] Ministry of Digital Policy, Telecommunications and Media, General Secretariat of Digital policy, Cyber Security, http://mindigital.gr/index.php/kyvernoasfaleia

[4] National Cyber Security Strategy, https://diavgeia.gov.gr/doc/474650-6?inline=true

[5] NIS Greek Law, https://www.taxheaven.gr/laws/law/index/law/908