European network of Cybersecurity centres and competence Hub for innovation and Operations

Project Overview

Notis Mengidis (nmengidis@iti.gr)
CERTH / ITI

Thessaloniki, 19 July 2019

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 830943

ECHO at a glance

- ECHO Governance model
  - Overall budget: 15,987,285€
  - 30 existing partners
  - 6 Academic/Institutional
  - 7 Industrial cyber centres
- Engagements with new partners
  - **Minimum 15 new engagements**
  - **Access to** ECHO Early Warning System
  - **Participation in** Technology Roadmaps
- **Sustainable model** for long term operations

Challenges

- Challenges for EU
  - Retain and develop essential capacities to secure its digital economy, infrastructures, society, and democracy
  - Better align cybersecurity research, competences and investments
  - Step up investment in technological advancements to make EU's digital single market more cybersecure and overcome fragmentation of research
  - Master relevant cybersecurity technologies from secure components to trustworthy interconnected IoT ecosystems and to self-healing software
  - Support industries and equip them with latest technologies and skills to develop innovative security products and services and protect their vital assets against cyberattacks
  - Contribute to the objective of European strategic autonomy

Aims

- What ECHO aims to do ?
  - Propose, test, validate and exploit the setup of a cybersecurity competence network with central competence hub
  - Bring together cybersecurity R&D&I centres in Europe and engage in:
    - Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual-use), applications and services with a focus on horizontal technologies as well as on critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing);
    - Scaling up existing research with solutions that can be marketable;
    - Strengthening cybersecurity capacities across the EU and closing the cyber skills gap;
    - Supporting certification authorities.

Current weaknesses

ECHO consortium identified following weaknesses in current cybersecurity technologies and operations:

1. Lack of effective means to assess multi-sector technology requirements across security disciplines;
2. Lack of effective means to assess dependencies between industrial sectors;
3. Lack of realistic simulation environments for technology research and development, or efficient security test and certification;
4. Lack of an up-to-date cyberskills framework as a foundation for cybersecurity education and training;
5. Lack of effective means to share knowledge and situational awareness in a secure way with trusted partners.

Project overall objectives

- Objective 1: Network of cyber research and competence centres, with a central competence hub
  - Demonstrate a network of cyber research and competence centres, with a central competence hub, allied with work of ENISA, Europol and other EU agencies and bodies, and having a mandate for increasing participation through a new partner engagements model, including partnership with other networks funded under the same call.

Project overall objectives

- Objective 2: ECHO Governance Model

  - Analyse various research and innovation governance models leading to the delivery of an ECHO Governance Model for effective operational management of the ECHO Network of Competence Centres.
  - ECHO Governance Model addresses at minimum 5 interdependencies among the network of competence centres: including (i) management and coordination of multi-centre and multi-partner relationships; (ii) management of multi-sector cybersecurity opportunities; (iii) management of sector specific and transversal opportunities; (iv) development of cybersecurity technology roadmaps across security disciplines; and (v) definition of cyberskills references and curriculum.

Project overall objectives

- Objective 3: ECHO Multi-sector Assessment Framework
  - Develop and demonstrate a comprehensive ECHO Multi-sector Assessment Framework, providing the means to analyse transversal and inter-sectoral challenges and opportunities and supporting development of cybersecurity technology roadmaps.
  - Deliver a multi-sector assessment framework encompassing at least three (3) specific vectors including
    - (i) industrial analysis of inter-sector dependencies;
    - (ii) horizontal technology and security disciplines (e.g. cryptography, network security, application security, IoT/cloud security, data integrity and privacy, secure digital identities, security/crisis management, forensic technologies, security investigation, cyber psychology, bio-security, data mining for threat intelligence, together with the use of artificial intelligence, machine learning and big data analytics for cyber security, among others);
    - (iii) transversal security factors that are independent of sector or discipline (e.g., legal, ethical and societal factors; cyberskills development; or policies and regulations).

Project overall objectives

- Objective 4: Cybersecurity Technology Roadmaps
  - Analysis and derivation of relevant Cybersecurity Technology Roadmaps resulting from the application of the ECHO Multi-sector Assessment Framework applied against sector specific, inter-sector and transversal cybersecurity challenges and opportunities.
  - provide a set of tangible opportunities, encouraging partners to engage together in common research, development and innovation in next generation cybersecurity technologies, applications and services whose achievement would demonstrate mastery of these relevant cybersecurity technologies, including horizontal inter-sector technologies, cybersecurity disciplines and transversal factors.
  - The project includes early prototype research and development for selected high priority technology opportunities identified as part of these cybersecurity technology roadmaps. These early prototypes will then be used to demonstrate the advantages derived from the framework. These roadmaps will use the results of the work done by the cPPP on cybersecurity, notably its Strategic Research and Innovation Agenda.

Project overall objectives

- Objective 5: ECHO Cybersecurity Certification Scheme
  - Develop and demonstrate an effective and efficient ECHO Cybersecurity Certification Scheme, aligned with current ENISA efforts to establish an EU Cybersecurity Certification Framework that addresses sector specific and inter-sector issues.
  - Overcome fragmentation of EU research capacities and technology developments by providing a common means to support certification authorities with testing and validation. This will further enhance market potential of horizontal technologies and endorsement of cybersecurity technologies through a portfolio of sector specific certification schemes targeted to specific sectors.
  - Sector selection will be driven by the outcomes of the application of the ECHO Multi-sector Assessment Framework which will highlight priority areas for development of Technology Roadmaps and, hence also, technology cybersecurity certifications.

Project overall objectives

- Objective 6: ECHO Early Warning System
  - Conduct research and development tasks to deliver an operational ECHO Early Warning System providing a mechanism for partners to share incident and other cybersecurity relevant data to trusted partners within the ECHO Network.
  - Provides an enabling technology in support of the ECHO network operations, ensuring a secure and sustainable method of collaboration and communication among partners.
  - Means by which the ECHO network will be able to test, validate and exploit the organisational, functional, procedural and technological operational setup of the cybersecurity competence network and central competence hub.

Project overall objectives

- Objective 7: ECHO Federated Cyber Range
  - Conduct research and development tasks to deliver an operational ECHO Federated Cyber Range providing a realistic environment for hands-on training development; conduct innovative experimentation and exercises, research and prototype testing; and conduct cybersecurity certification testing.
  - Provides an enabling technology in support of the ECHO Network operations, ensuring a safe and reliable multi-sector simulation environment in which to ensure viable delivery of identified technology roadmaps, as well as, hands-on cyberskills development involving realistic sector specific or multi-sector simulations.

Project overall objectives

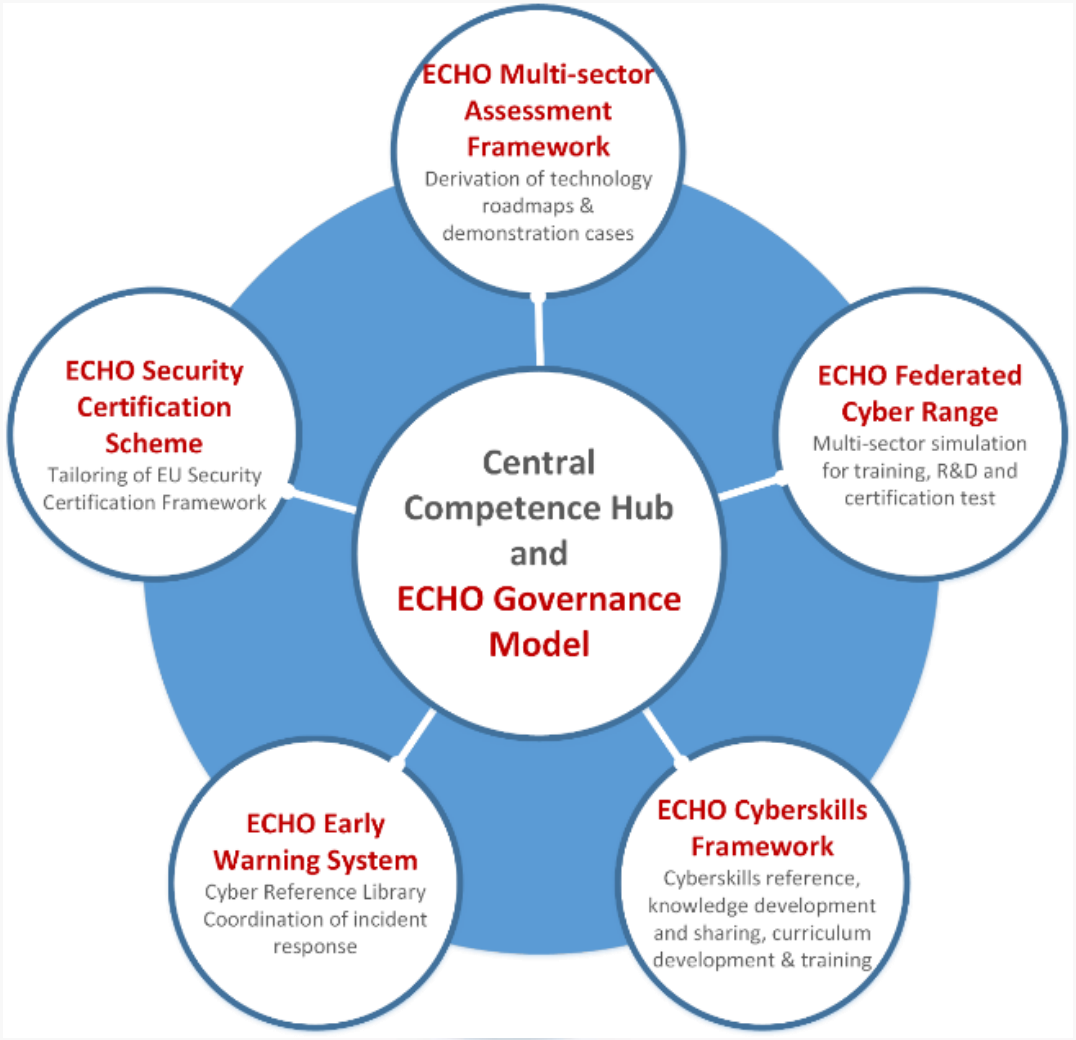
- Objective 8: Demonstration Cases
  - Develop a collection of Demonstration Cases that will highlight the value of synergies developed by the ECHO Network including demonstrations supporting inter-sector synergies and opportunities for full life-cycle support to delivery on identified technology roadmaps.
  - Highlight the opportunities derived from the ECHO Network for partners to engage together in common research, development and innovation in next generation cybersecurity technologies, applications and services.
  - Promote the use of the ECHO EWS and ECHO FCR, as these enabling technologies themselves are results of the collaborative potential enabled by the ECHO Network.
  - Collectively develop and implement the previously described Cybersecurity Technology Roadmaps addressing multiple and complementary cybersecurity disciplines.

Project overall objectives

- Objective 9: ECHO Cyberskills Framework
  - Analysis and derivation of ECHO Cyberskills Framework and related training and education calendar and curriculum resulting from application of the ECHO Multi-sector Assessment Framework applied against sector specific, inter-sector and transversal cybersecurity challenges and opportunities.
  - Contribute to achieve European strategic autonomy and help build and strengthen cybersecurity capacities across the EU through delivery of a common reference model for cyberskills.
  - Develop and pilot collection of cyber curricula involving training that spans both strategic and policy aspects as well as technology-oriented aspects.
  - Participation in the ECHO Network will allow existing member of the ECHO consortium to engage together, as well as with new partners, colleagues from other competence networks, the EU and other agencies in strengthening cybersecurity capacities and closing the cyber skills gap.

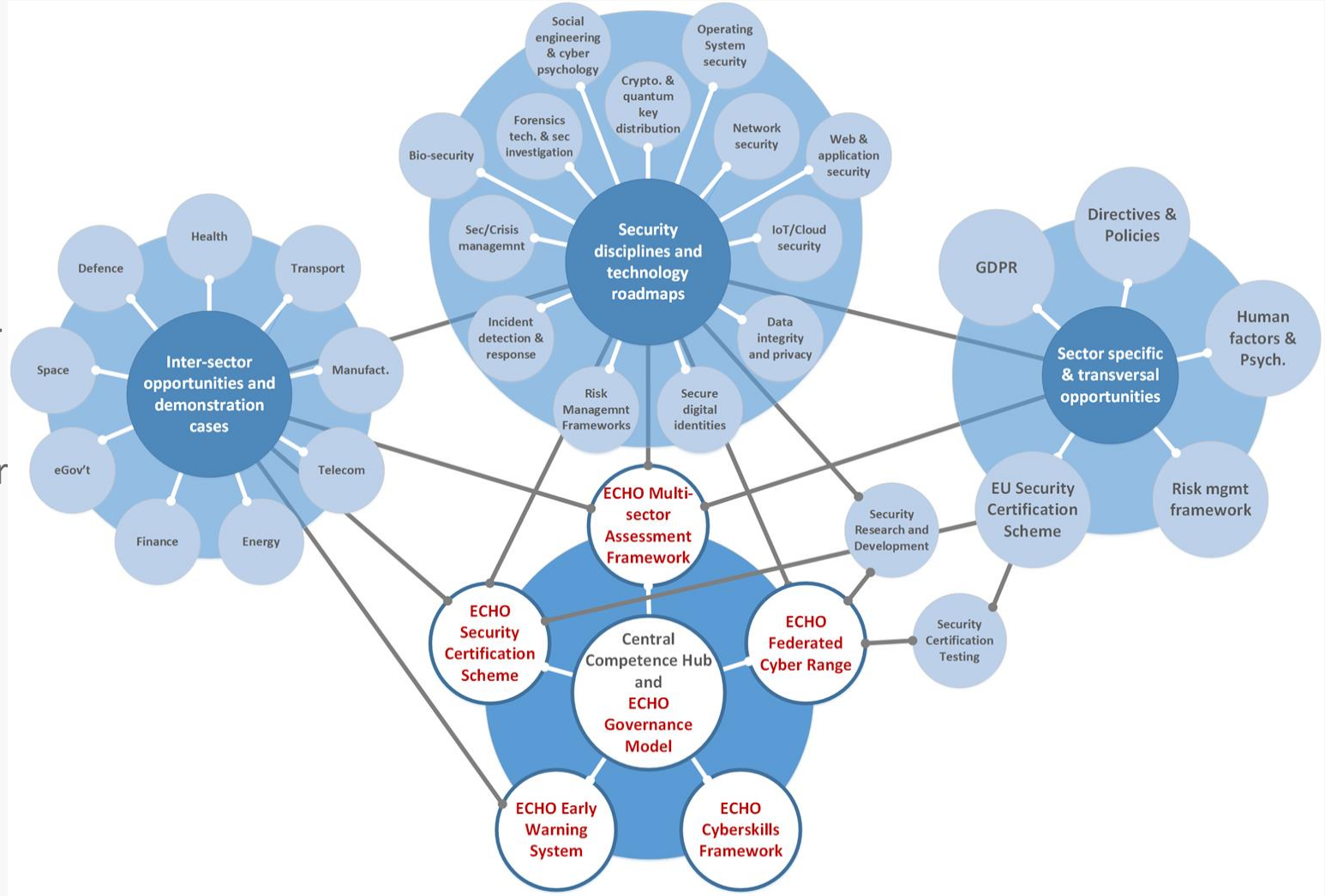
Innovations and Impact

- Main Innovations:
  - **ECHO Governance Model:** Management of direction and engagement of partners (current and future)
  - **ECHO Multi-sector assessment framework:** Transverse and inter-sector needs assessment and technology R&D roadmaps
  - **ECHO Cyberskills Framework and training curriculum:** Cyberskills reference model and associated curriculum
  - **ECHO Security Certification Scheme:** Development of sector specific security certification needs within EU Cybersecurity Certification Framework from ENISA
  - **ECHO Federated Cyber Range:** Advanced cyber simulation environment supporting training, R&D and certification
  - **ECHO Early Warning System:** Secured collaborative information sharing of cyber-relevant information



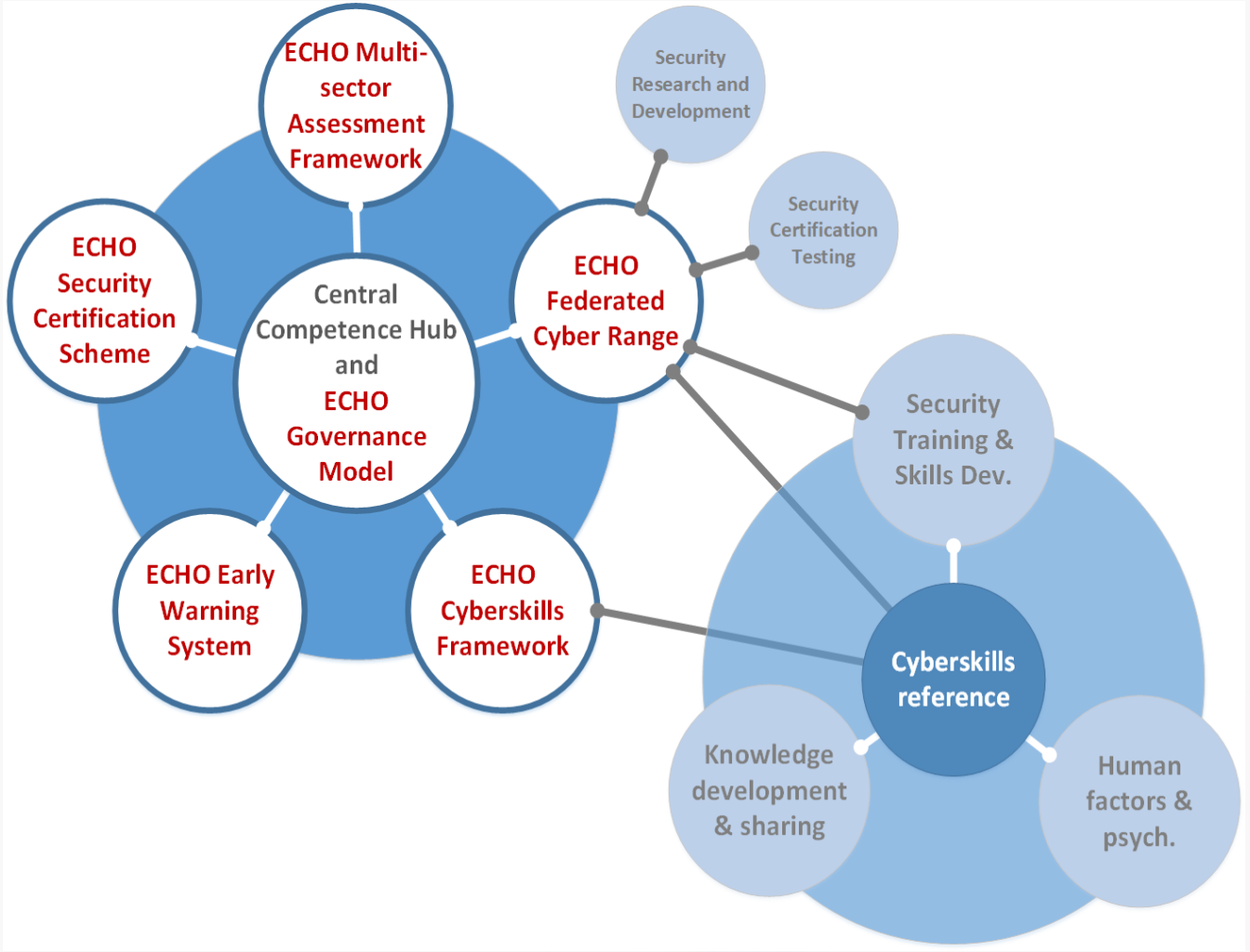
Innovations and Impact

- ECHO Multi-sector assessment framework
  - Mechanism to define and refine **technology roadmaps** and **demonstration cases**
- Risk based method to analyse multi-sector security needs including:
  - **Inter-sector opportunities** (potential solutions) to security challenges further analysed as **demonstration cases**
  - Comprehensive analysis of potential contributions to **technology roadmaps** across **security disciplines** as means to improve security posture
  - Analysis of **sector specific needs** and **transversal opportunities** to identify potential for improvement



Innovations and Impact

- ECHO Cyberskills framework
  - Mechanism to improve the **human capacity** of cybersecurity across Europe
- Leverage a **common cyberskills reference**:
  - Derived and refined from ongoing and related work (e.g, ECSO, e-Competence Framework, European Qualification Framework)
- Design modular **learning-outcome based curricula**
- **Hands-on skills development** opportunities through realistic simulation (ECHO Federated Cyber Range)
- Lessons learned feed **knowledge sharing** (ECHO Early Warning System)



Innovations and Impact

- ECHO Federated Cyber Range
  - Interconnect existing (X 7) and new cyber range capabilities through a convenient portal
  - Portal operates as a **broker** among cyber ranges
  - Enables access to emulations of **sector specific and unique technologies**
- Cyber Range is a multipurpose **virtualization environment** supporting **"security-by-design"** needs
  - Safe environment for **hands-on cyberskills** development
  - Realistic simulation for **improved system assurance** in development
  - Comprehensive means for **security test and certification** evaluation
- To be used as virtual environment for:
  - Development and demonstration of **technology roadmaps**
  - Delivery of specific instances of the **cyberskills training** curricula

Innovations and Impact

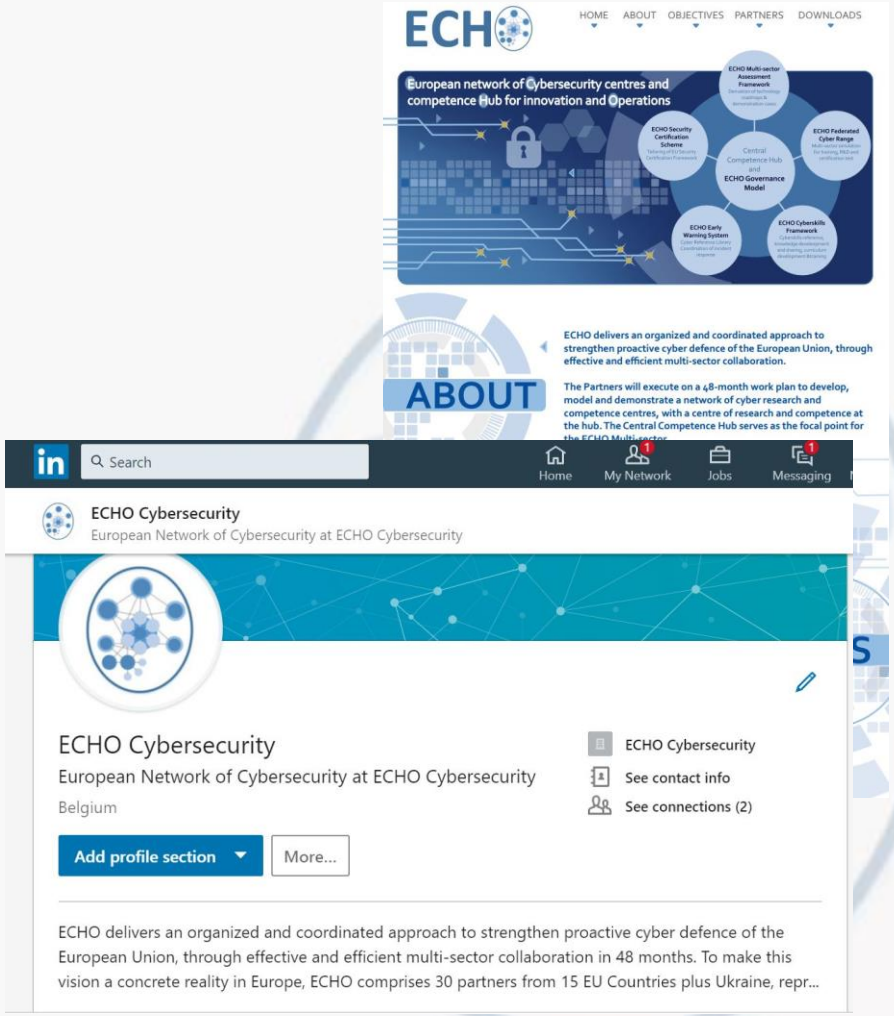
- ECHO Early Warning System
  - **Security operations support** tool enabling members to **coordinate and share** cyber relevant information in near-real-time
  - Secure information sharing **between organizations**; across organizational boundaries and national borders
  - Coordination of **incident management workflows**
  - Retain **independent management and control of cyber-sensitive** information
  - Account for **sector specific needs** and protection of **personal information protection** (GDPR compliant)
  - Includes sharing of **reference library** information and **incident management** coordination

Innovations and Impact

- ECHO Cybersecurity Certification Scheme
  - Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)
  - Provide **product oriented** cybersecurity certification schemes
    - Support sector specific and inter-sector security requirements
  - Support **delivery and acceptance of technologies** resulting from technology roadmaps
    - **Improved security assurance** through use of **certified products**
  - Support development of **Digital Single Market**
    - Limits duplication and fragmentation of the cybersecurity market
    - **Common** cybersecurity **evaluation methods, acceptance** throughout Europe
    - Applicability across **Information Technologies** (IT/ICT) and **Operations Technologies** (OT/SCADA)

Social Media

- ECHO website: www.echonetwork.eu
- Twitter: **@ECHOcybersec**
- Linkedin: [ECHO cybersecurity]
- For information: info@echonetwork.eu



Thank you!
Questions?