ECHO Project Overview

Matteo Merialdo
Project Implementation Coordinator

05 November 2019

RHEA Group

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

Cybersecurity Gaps for EU

ECHO consortium identified gaps in current cybersecurity technologies and operations in EU:

1. Lack of effective means to assess multi-sector technology requirements across security disciplines
2. Lack of effective means to assess dependencies between different 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

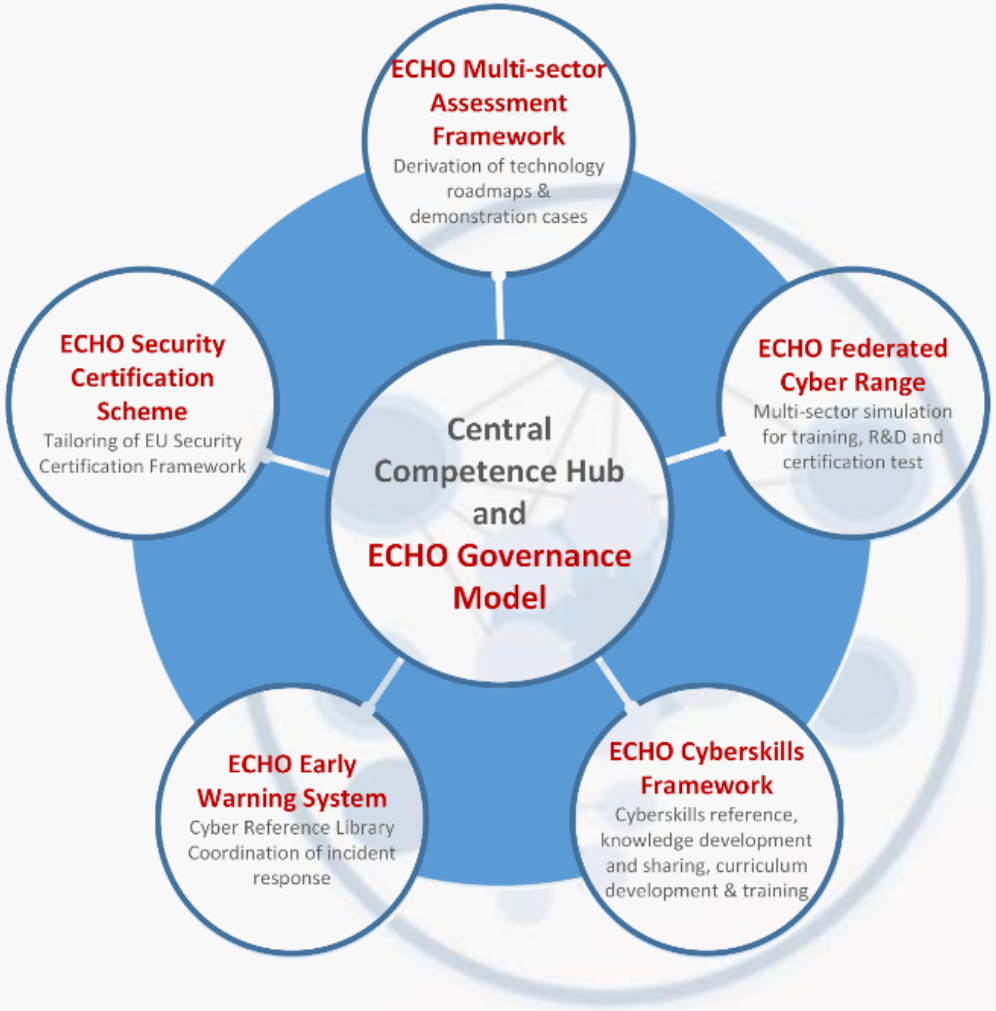
These gaps **are particularly relevant for EU**

ECHO main objectives

- 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, having a mandate for increasing participation through a new partner engagements model, including collaboration with other networks funded under the same call
  - Address all the aforementioned gaps, developing an adaptive model for information sharing and collaboration among the network of cybersecurity centres, supported by an early warning system and a framework for improved cyberskills development and technology roadmap delivery, in a multiple-sector context

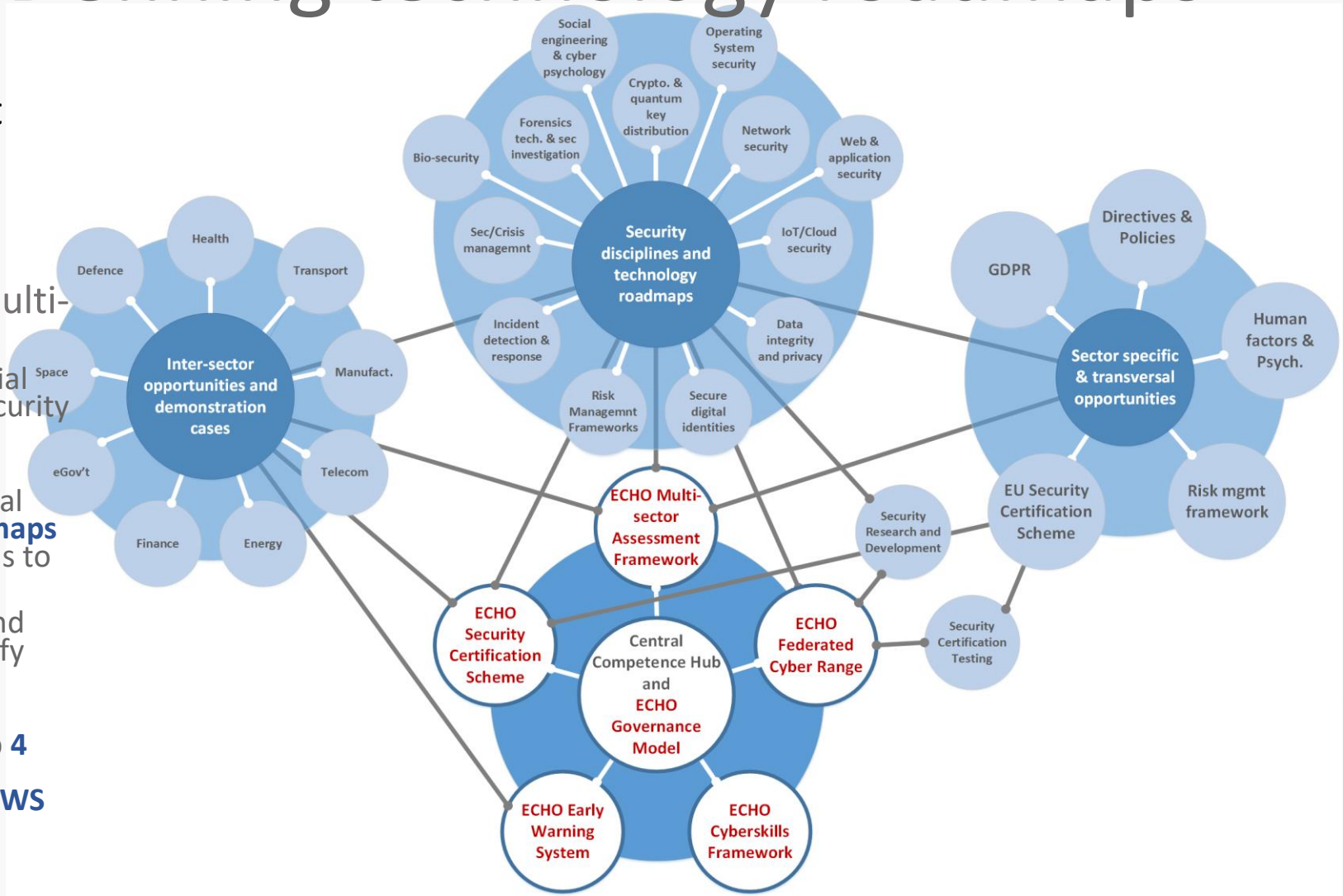
European network of Cybersecurity centres and competence Hub for innovation and Operations

- Project Coordinator: **Royal Military Academy of Belgium (Wim Mees)**
- Project Management: **RHEA System S.A. (Matteo Merialdo)**
- Main concepts:
  - 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
  - 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



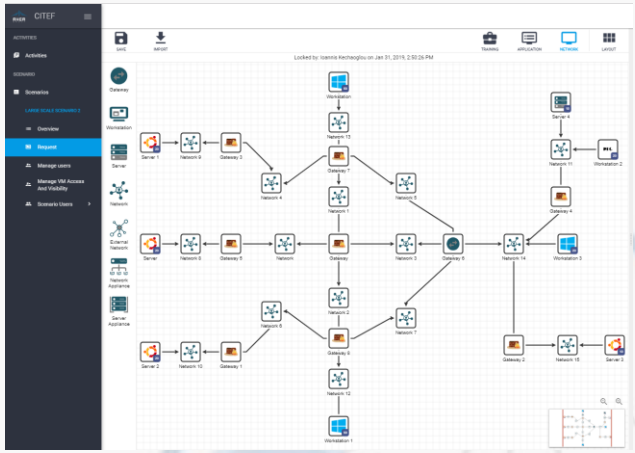
Defining technology roadmaps

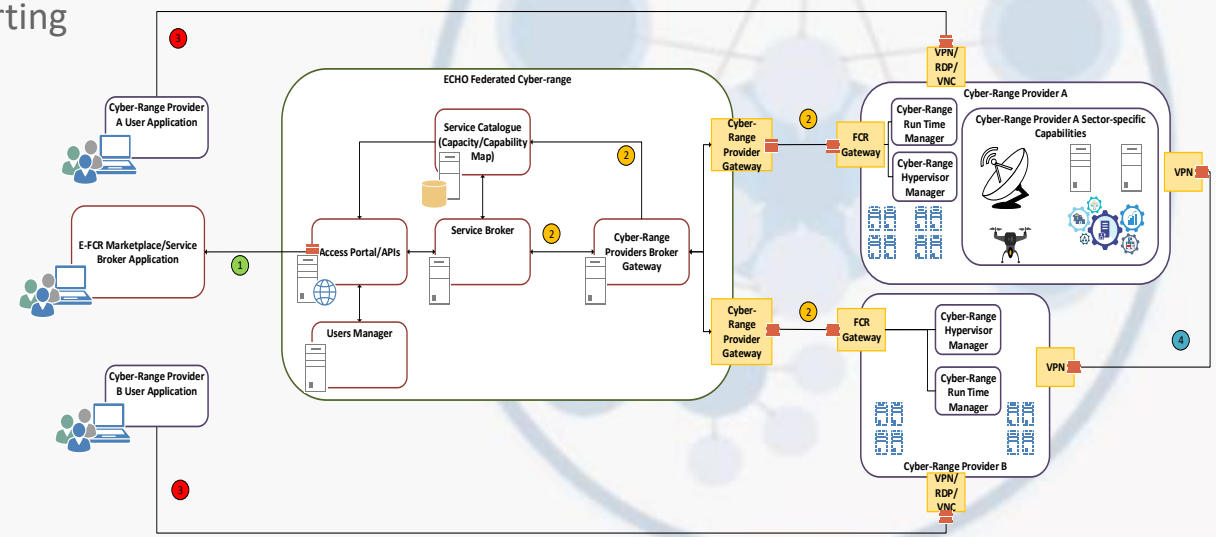
- ECHO Multi-sector assessment framework
  - Mechanism to define and refine **technology roadmaps** and **demonstration cases**
- Risk based method to analyse multi-sector security needs including
  - **Inter-sector opportunities** (potential solutions) and **dependencies** to security challenges further 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
  - ECHO targets to identify at least **6 technology roadmaps** and develop **4 technology innovations** on these roadmaps, including **E-FCR and E-EWS**



Technology roadmap: E-FCR

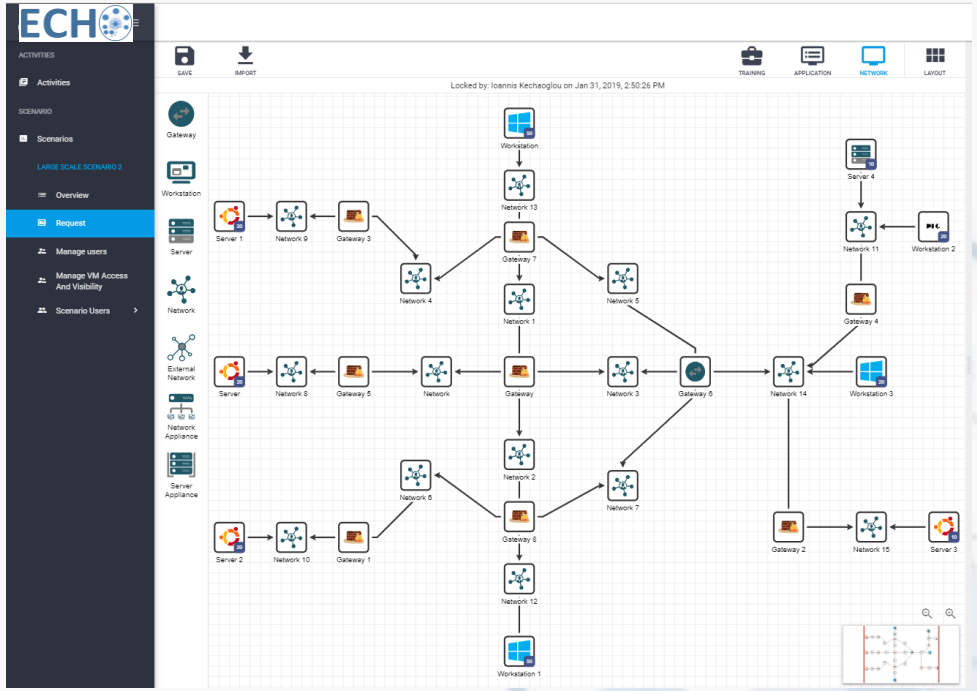
- ECHO Federated Cyber Range (FCR)
  - Interconnect existing and new cyber range capabilities through a convenient portal
  - Portal operates as a **broker** among cyber ranges
  - A **marketplace** enable content providers to sell cyber range contents to a wider market
  - Enables access to emulations of **sector specific and unique technologies**
  - Target **Technology Readiness Level: 8**
  - Governance Model in development
- 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





E-FCR concept

- Customers will have access to
  - Service Designer -> concept already in progress (develop new scenarios leveraging on single or multiple ranges)
  - Marketplace (content providers can upload contents/scenarios for a wider market)



amazon

Acumos

Technology roadmap: E-EWS

- 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
  - Target **Technology Readiness Level: 8**
  - Governance and Sharing Models in development

Outcomes

- ECHO targets practical use of outcomes to offer technologies and services having increased cyber-resilience by sector and among inter-dependent partners
  - Use of E-FCR for experimental simulation of cyber-attack scenarios, pre-production testing, product evaluations
  - Combined use of E-FCR and E-Cybersecurity Certification Scheme (E-CCS) for certified qualification testing of potential technologies required to meet customer specification
  - Use of E-CCS as benchmark of cybersecurity certification to be obtained as a market differentiator
  - Use of E-EWS to share early warning of cybersecurity related issues (e.g., vulnerabilities, malware, etc..)
  - Promotion of improved cyberskills through leveraging diverse education and training options made available by the E-Cybersecurity Skills Framework, particularly as it relates to security-by-design best practices
- Although not clear what will be the future of the 4 Pilot projects, it is expected the most relevant outcomes will be merged to create the **future EU cybersecurity competence centres network**

Partners

Key summary

- 30 partners
- 15 new partner engagements
- 13 existing competence centres
- 16 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios

Social Media

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

- Youtube: https://www.youtube.com/channel/UCDQBXrQhoLJ2lnf38x1X6Uw