European network of **C**ybersecurity centres and competence **H**ub for innovation and **O**perations

22 January 2020

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

Introduction

European strategic autonomy & cybersecurity

- 18 EU countries jointly stated that the EU must “ensure its technological autonomy by supporting the development of a digital offer and create global reference players”, Paris, 18/12/2018

Identified challenges for the upcoming years

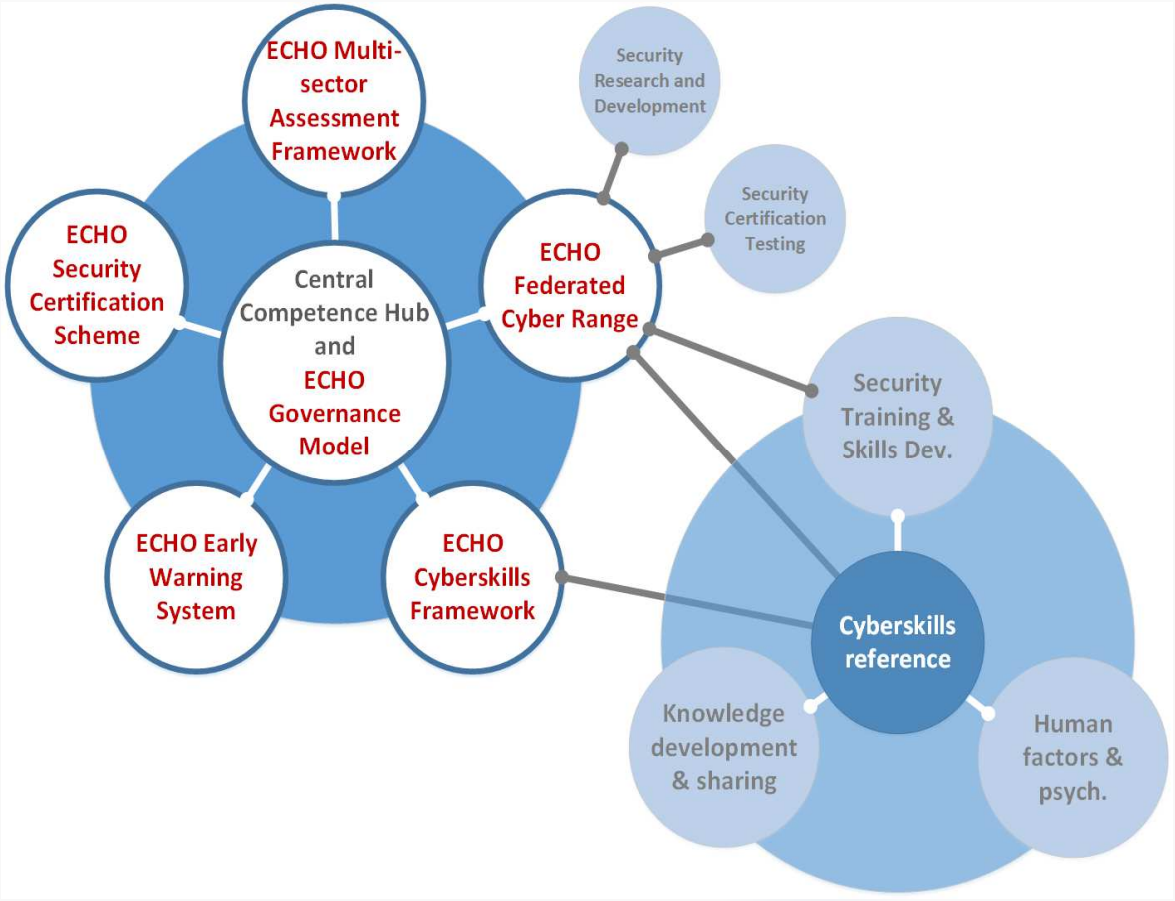
- Retain and develop essential capacities
- Better align cybersecurity research, competences and investments
- Step up investment in technological advancements to make EU's digital single market more cybersecure and overcome fragmentation of research

Main ECHO objectives (focus)

- ECHO Cyberskills framework (leverage on ESCO)
- ECHO Security Certification Scheme
- ECHO Early Warning System
- ECHO Federated CyberRange

ECHO Cyberskills and curricula

- 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)



ECHO Cybersecurity Certification Scheme

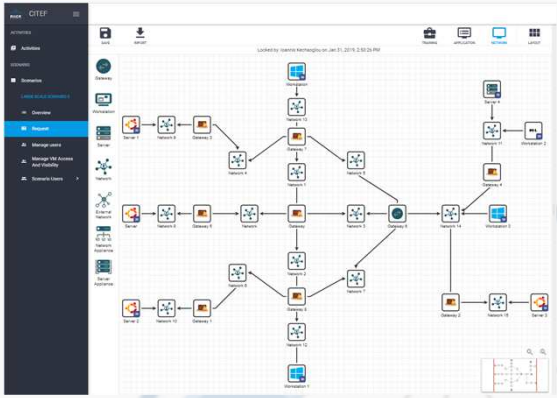
- Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)
- Provide **product oriented** cybersecurity certification schemes
  - Support sector specific and inter-sector security requirements
- Support **delivery and acceptance 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)

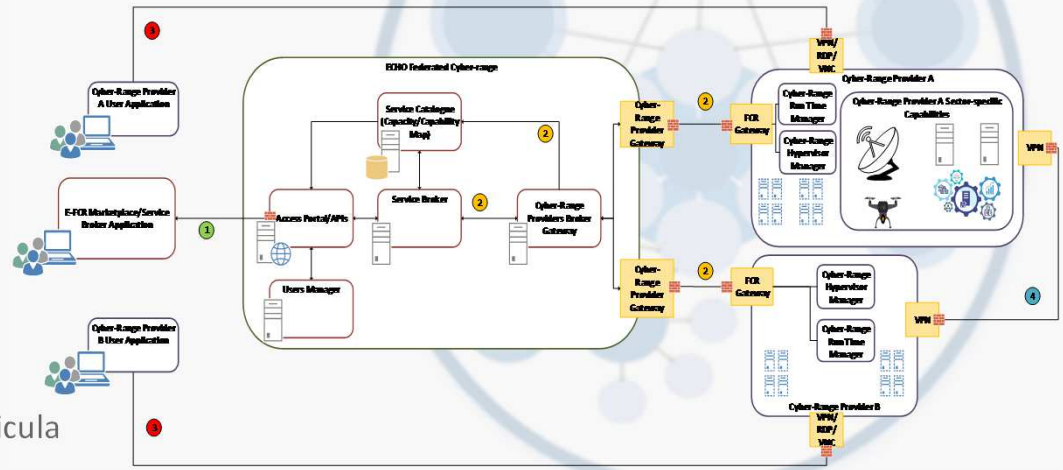
ECHO Technology roadmap: E-EWS

- 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: 9**
  - Governance and Sharing Models in development
  - **Potentially, it could serve all the network of centres of competeces!**

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





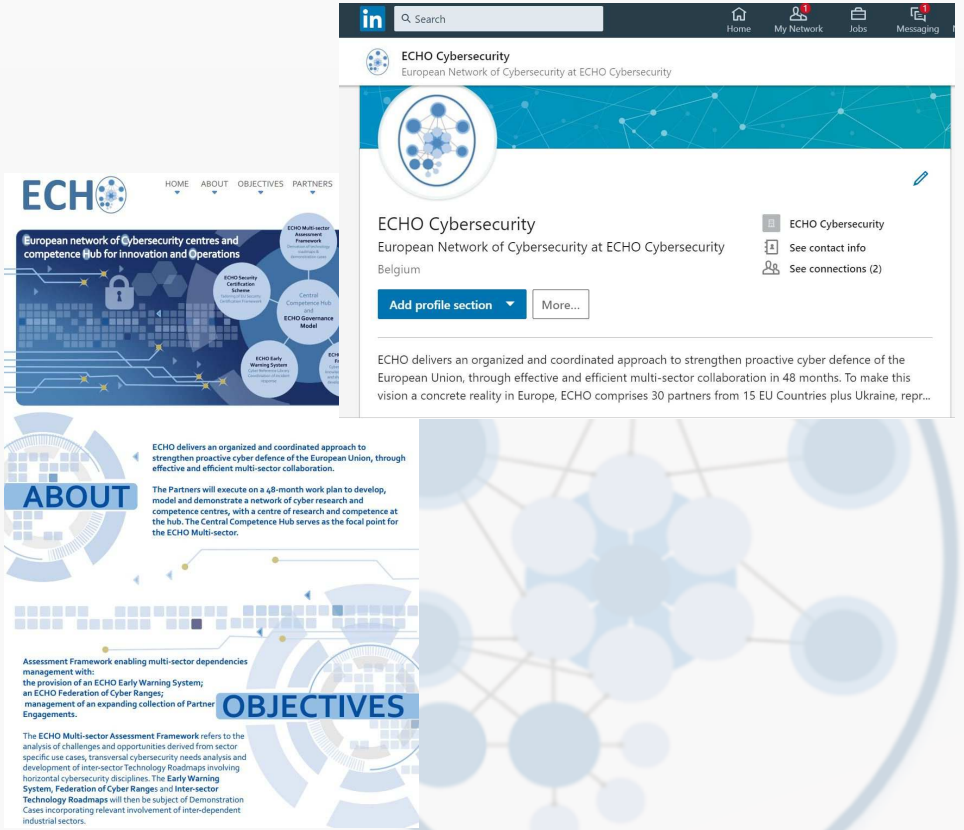
Partners

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

Thank you for paying attention, any question ?

→ ECHO or active consortiums : gregory.depaix@naval-group.com

22 January 2020

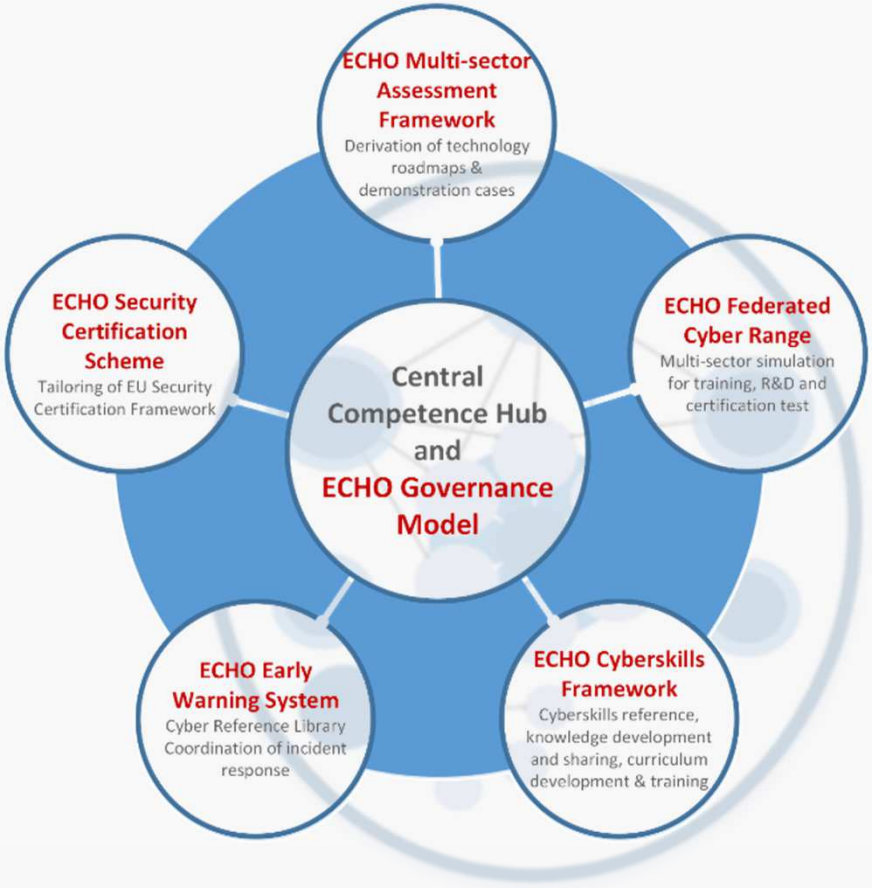
→ Calls connected to Cyber (&& ||) maritime: SU-AI-02-2020, SU-DS-04-2020, SU-DS-02-2020, SU-INFRA-01-2020

→ patrick.hebrard@naval-group.com and fabien.lacoste@naval-group.com

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

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

- 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



Project Structure