ECHO Generic Presentation

Matteo Merialdo
Manager, Security Research and Development (R&D) Projects at RHEA

ECHO Project Implementation Coordinator

17 January 2020

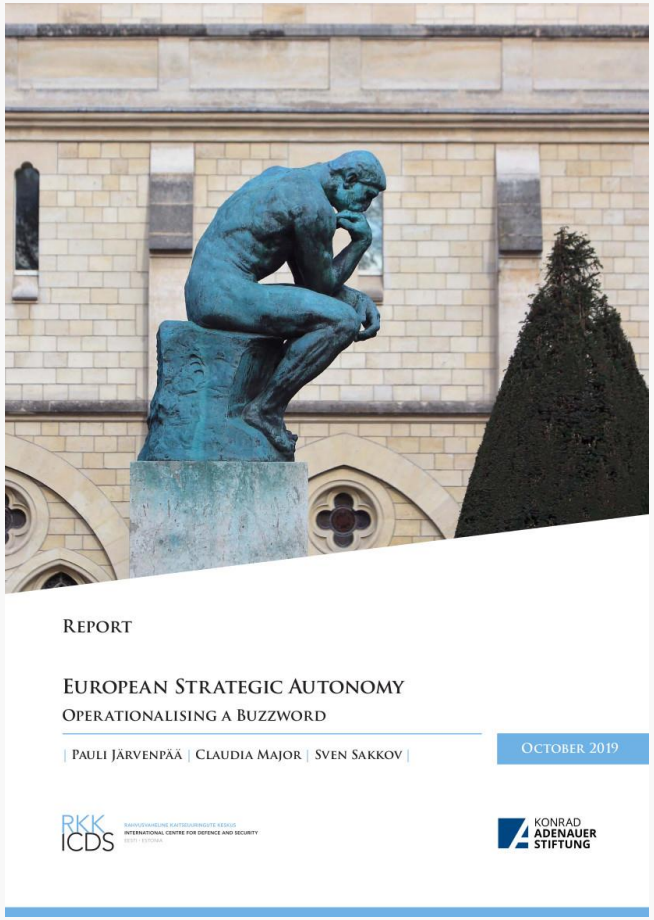
RHEA Group

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

The EU cybersecurity challenge

from *“fragmented in diversity”* to *“united in diversity”*

European strategic autonomy



- The capacity to act in four dimensions:
  - Political
  - Institutional
  - Capabilities
  - Industrial

European strategic autonomy and cybersecurity

Friends of Industry

6th Ministerial Meeting

Paris, Tuesday 18th december 2018

Joint statement by

France, Austria, Croatia, Czech Republic, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Luxembourg, Malta, Netherlands, Poland, Romania, Slovakia, Spain

Industry is a key driver for growth. It forms the backbone of the European economy and its long-term competitiveness. It employs around 32 million people in Europe and an additional 30 million in industry-related sectors.

Our industry is facing increasing fierce competition from other major economic blocks, which are developing their own proactive industrial strategies. Global trade environment is currently undergoing important trouble and European industry tends to suffer from increasingly protectionist trade measures from third countries.

European industry is, in fact, at a crossroads. We must act quickly to maintain its competitiveness, while taking into account the energy transition to a safe, sustainable and low-carbon and circular economy and the digital transformation of the industry.

1/ We call for a new political impetus in favour of industry at European level to face these challenges

As stated in the Competitiveness Council Conclusions adopted under the Austrian Presidency, the European Union (EU) must adopt a comprehensive vision for its industrial policy, in order to strenghten its strategic autonomy and meet the major challenges ahead, such as the transition to a digital and safe, sustainable, low-carbon and circular economy in accordance with the Paris Agreement under the United Nations Framework Convention on Climate Change, strategic access to raw materials as well as feedstocks, and affordable energy prices.

The industrial strategy should take into account the need for reindustrialisation and the differences in the industrial base development among Member States. It should therefore offer instruments tailored to the needs of industries and regions concerned, thus improving the competitiveness of the entire Union.

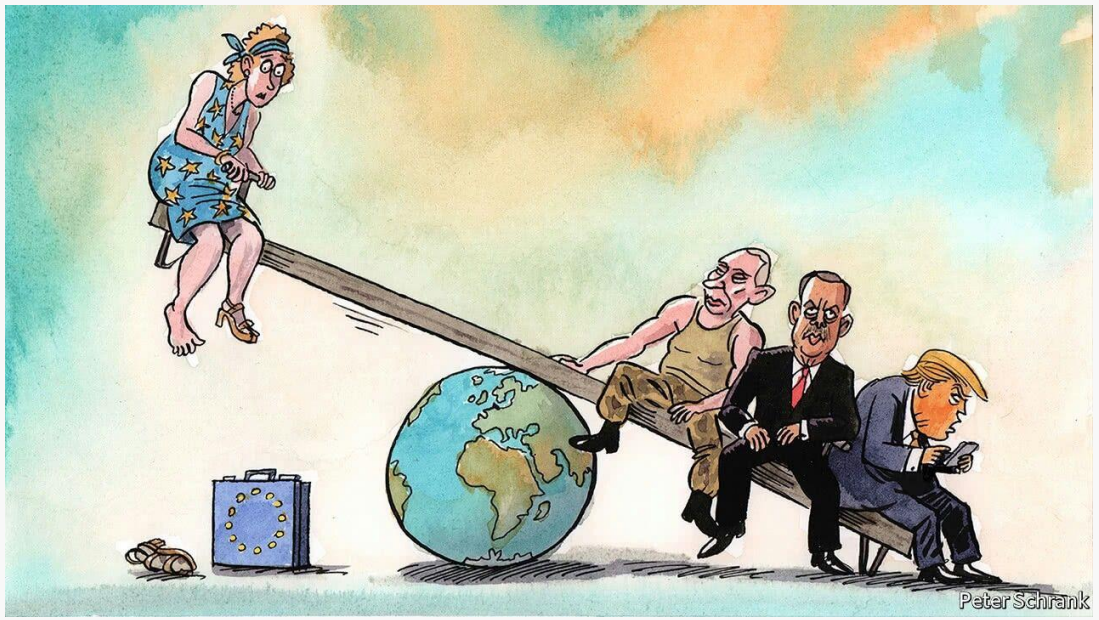
Identifying the strategic value chains of the EU is an important first step towards the setting of conditions favourable to innovation, investment and to the development of a European industrial leadership among the global value chains.

2/ Our ambition for an assertive industrial policy is articulated around four objectives

- ***Objective 1*: Obtain that the new European Commission, as soon as it is in place, propose an ambitious and comprehensive industrial strategy based on priority objectives to be reached by 2030** as a part of EU long-term strategy. Such strategy shall mobilise all European policies and all departments of the European Commission in order to contribute to reducing the regulatory burden on European industry, in particular for SMEs and small mid-caps, and

- 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**”

Our strategic autonomy focus for cybersecurity



- Strategic autonomy must be:
  - Sustainable
    - **Governance model**
    - Bottom-up input to decision makers
  - Technology driven
    - From recognized European scientific excellence to a trusted supply chain of **industrialized solutions**
  - Capability driven
    - Autonomy to **assess a situation**, **make decisions** and freedom of action to execute them

Cybersecurity Challenges for EU

Cybersecurity challenges have been identified by the EC for the upcoming years

- 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

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**

Industrial and technological challenges

- No one-size-fits-all solutions
- Develop a multi-sector assessment framework
- Identify sector specific, inter-sector and transversal opportunities
- Define a number **of technology roadmaps** and **demonstration cases**
- **Sets priorities for a number of other ECHO activities**

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

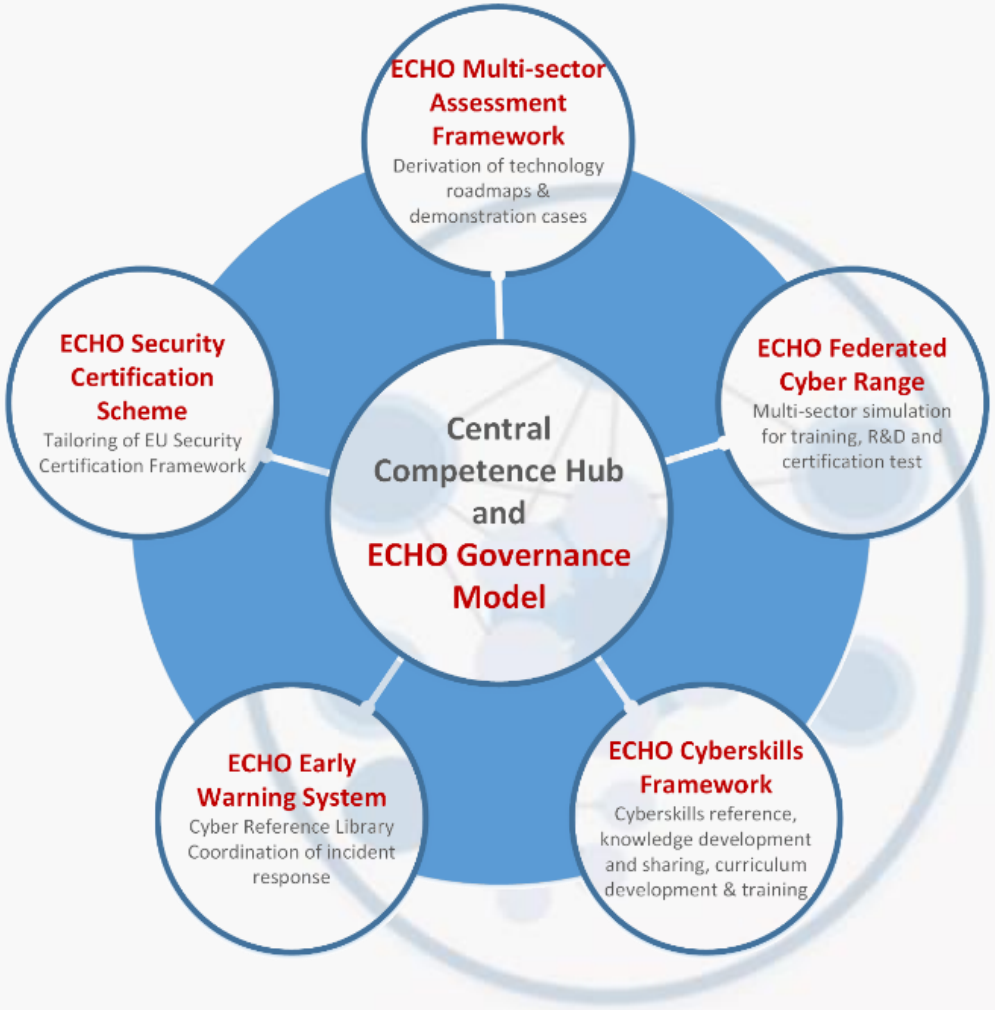
Partners

Key summary

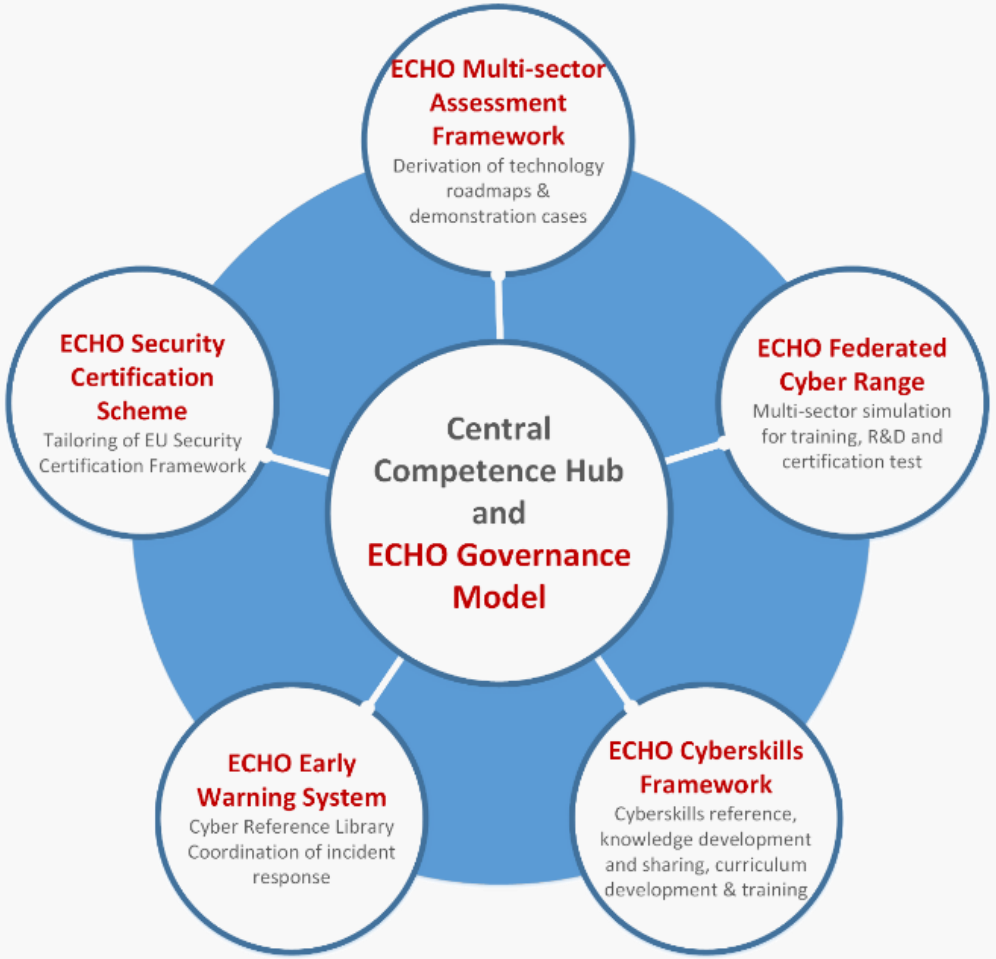
- Project Coordinator: **Royal Military Academy of Belgium (Wim Mees)**
- Project Management: **RHEA System S.A. (Matteo Merialdo)**
- 16 Millions budget (1.7 for RHEA)
- 4 years (started Feb 2019)
- 30 partners
- 15 new partner engagements
- 13 existing competence centres
- 16 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios

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



ECHO Governance Model



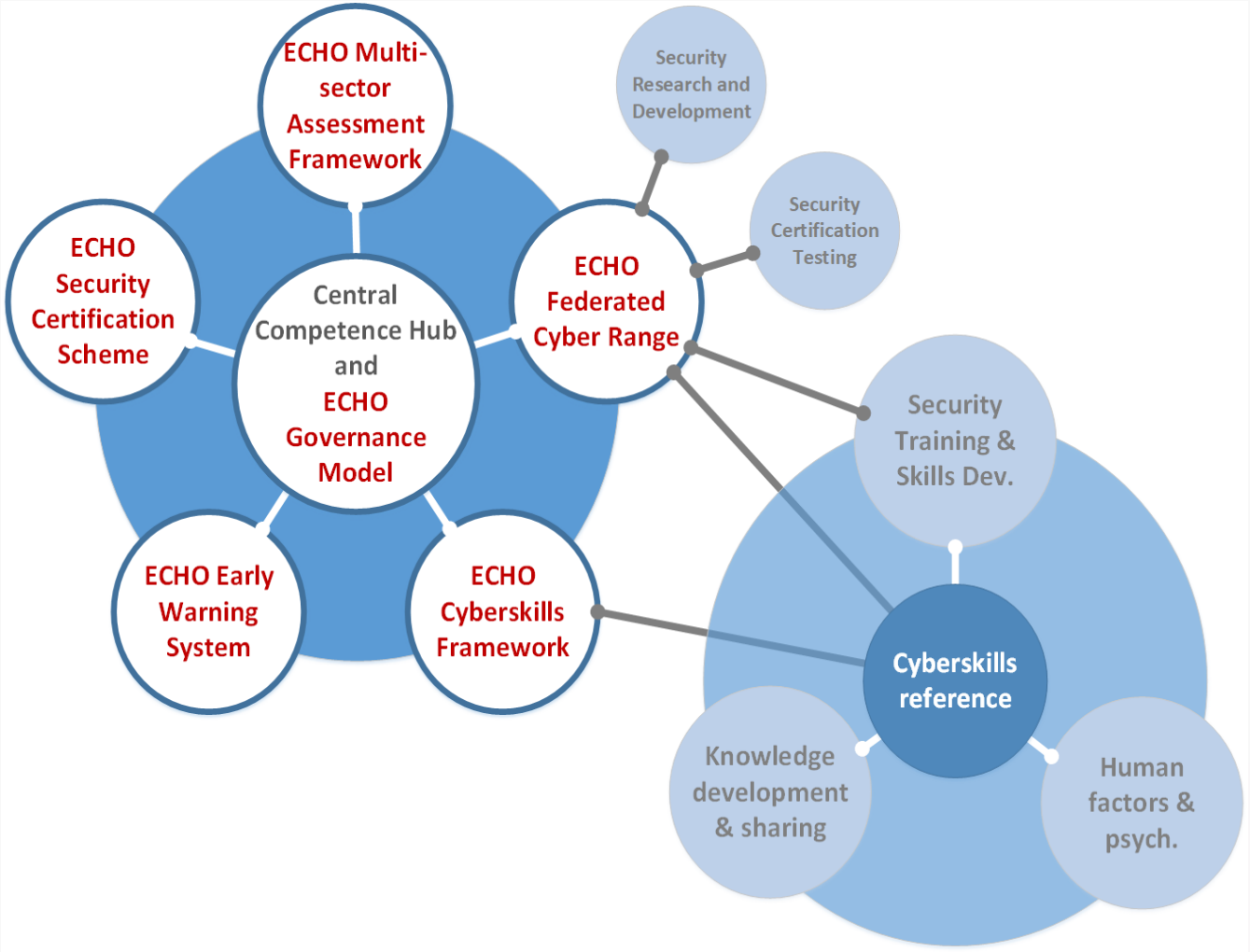
- Identify potentially applicable existing models
- Identify and prioritize governance needs
- Identify the most suitable governance model
- Define the governance model for the future Network of Centres of Competences
- Grow the network

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**

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

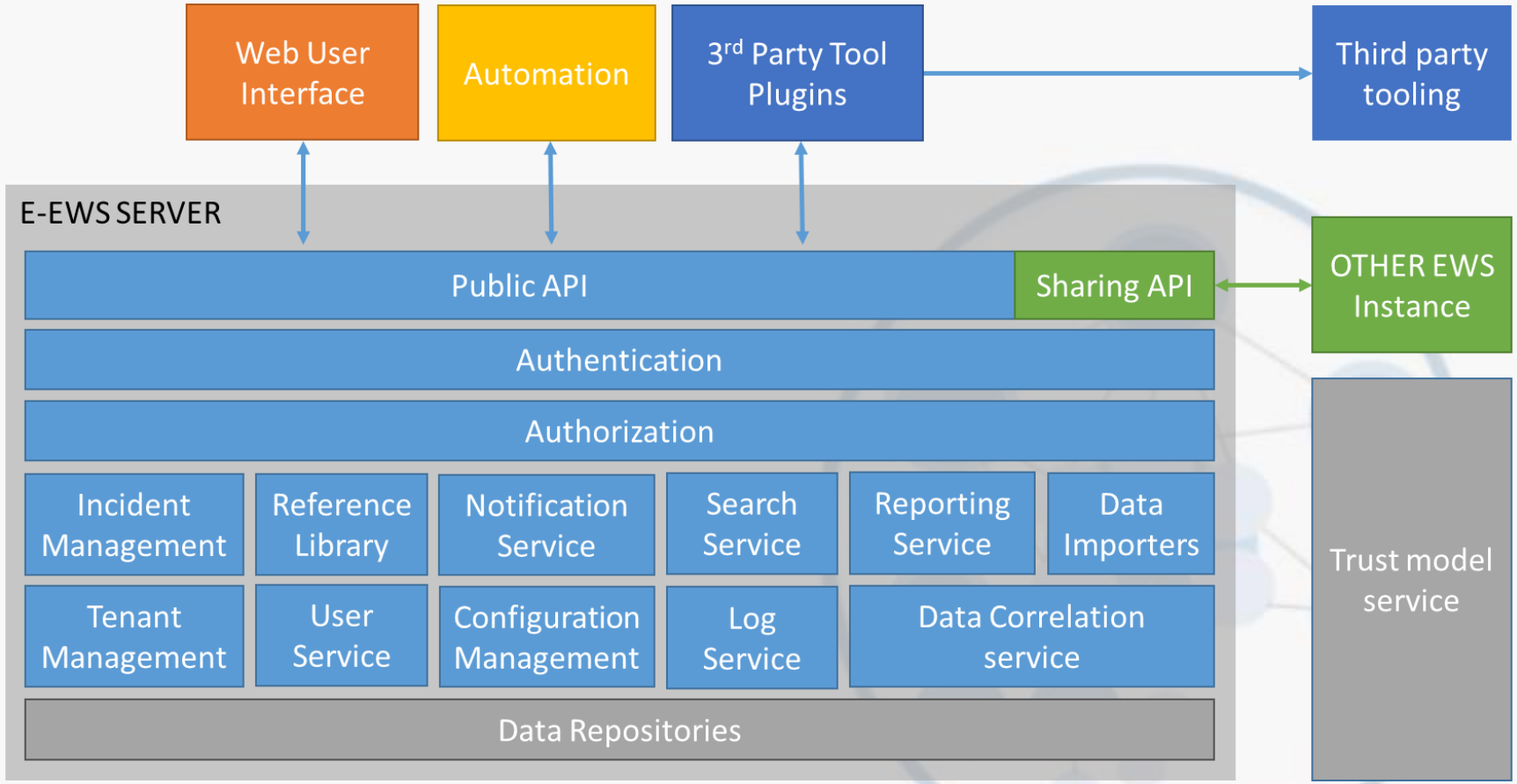
- Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)
- Provide **product oriented** cybersecurity certification schemes
  - Support sector specific and inter-sector security requirements
- Support **delivery and acceptance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

E-EWS Concepts

- Plugins for:
  - Integration with other standards / tools
  - Automation of CSIRT processes
  - Data analysis (e.g. predictive analytics)
  - Incident detection
- Objectives:
  - Create an eco-system (starting with partners developing plugins)
  - Develop a governance scheme for a distributed EWS
  - TRL 9

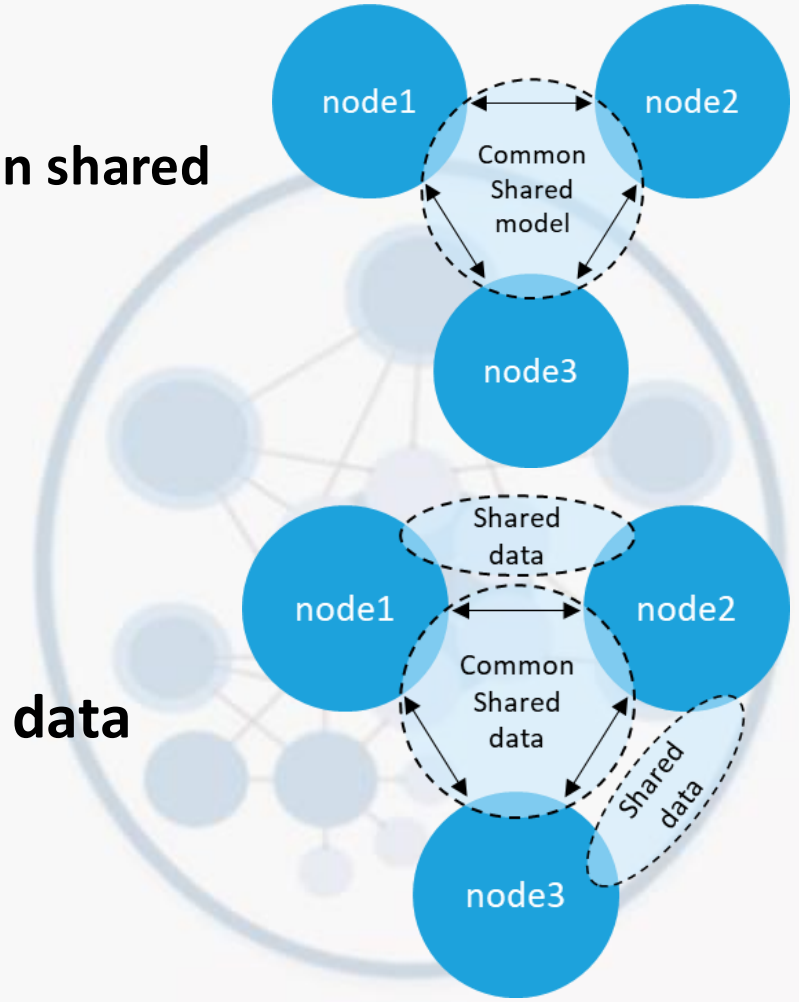


E-EWS Concepts

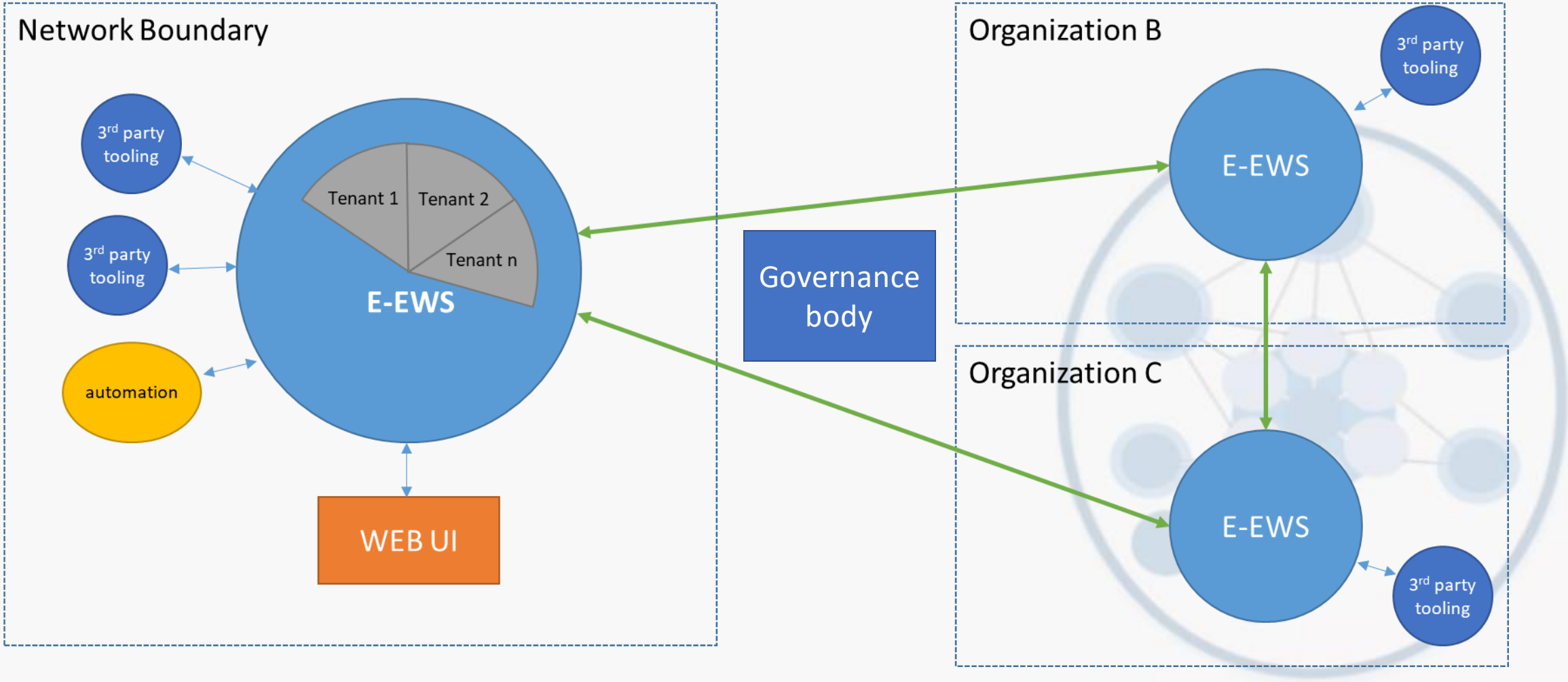
- E-EWS Server
  - The server installation or the E-EWS supports the main functionality of the system.
  - Exposes the APIs for public interaction
  - Fully owned by RHEA, with **CIRP** Technology
- Web User Interface
  - The main user interface in support of the E-EWS functionalities
  - Used by the EWS operators
  - Makes use of public API
- Automation
  - Allow tooling to be automated by E-EWS data
  - Makes use of public API
- 3rd Party Tool Plugins
  - Support 3rd party tooling to interact with E-EWS
  - Plugin architecture to allow independent development
  - Plugin acts as a bridge/mapping between the tooling API and the E-EWS
  - Makes if of public API
  - Trust Model

Common shared model

Shared data

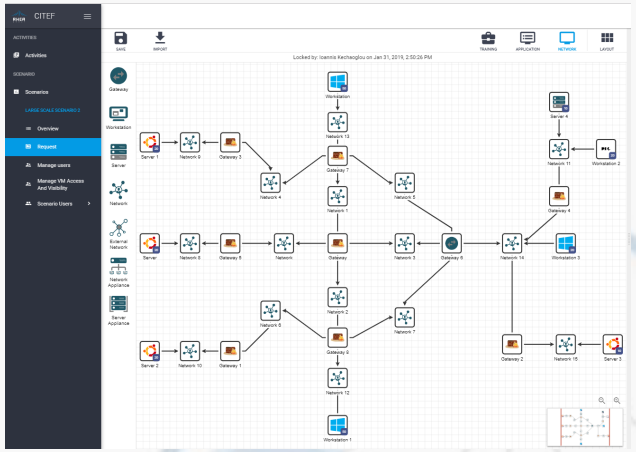


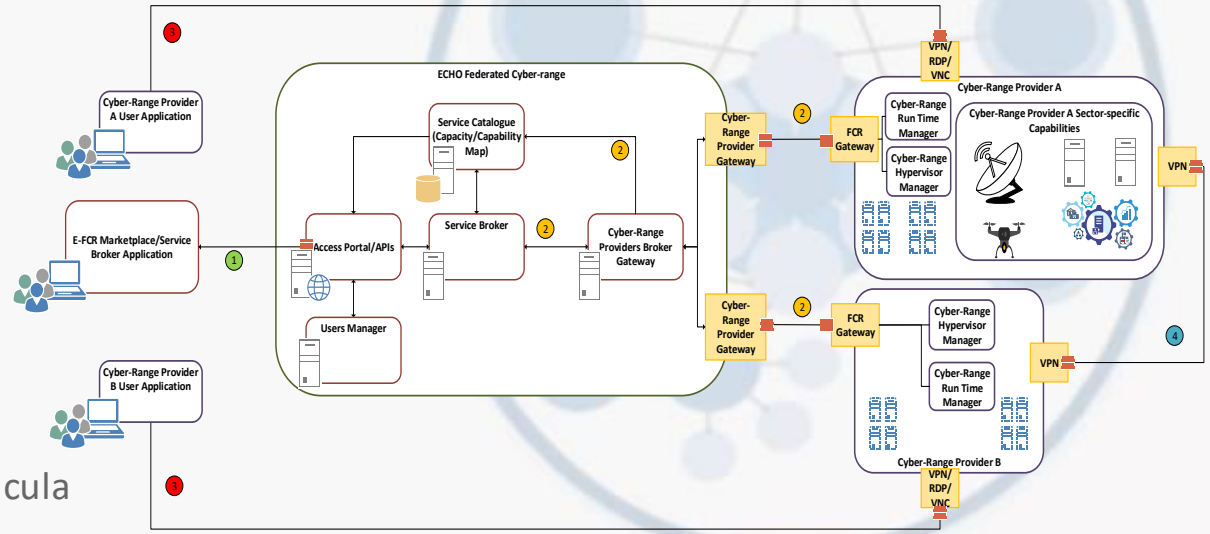
E-EWS concepts - distribution



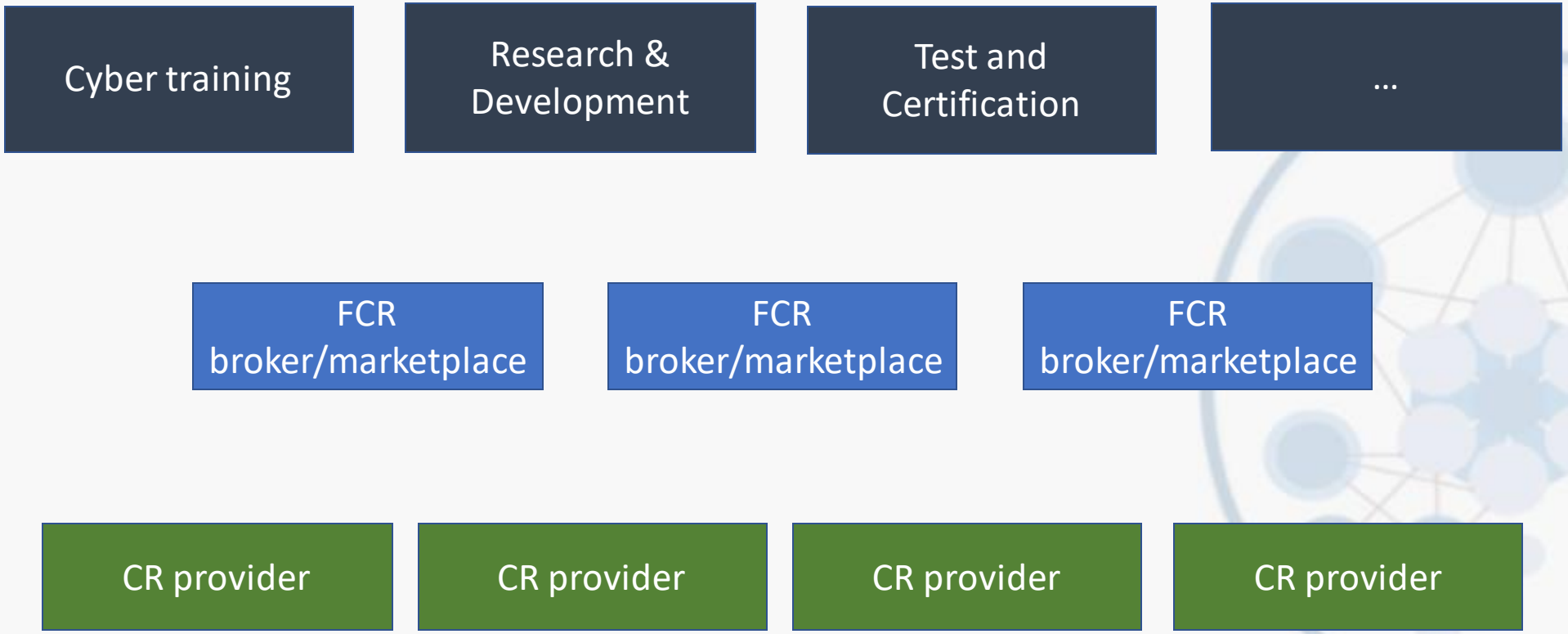
Technology roadmap: E-FCR

- 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



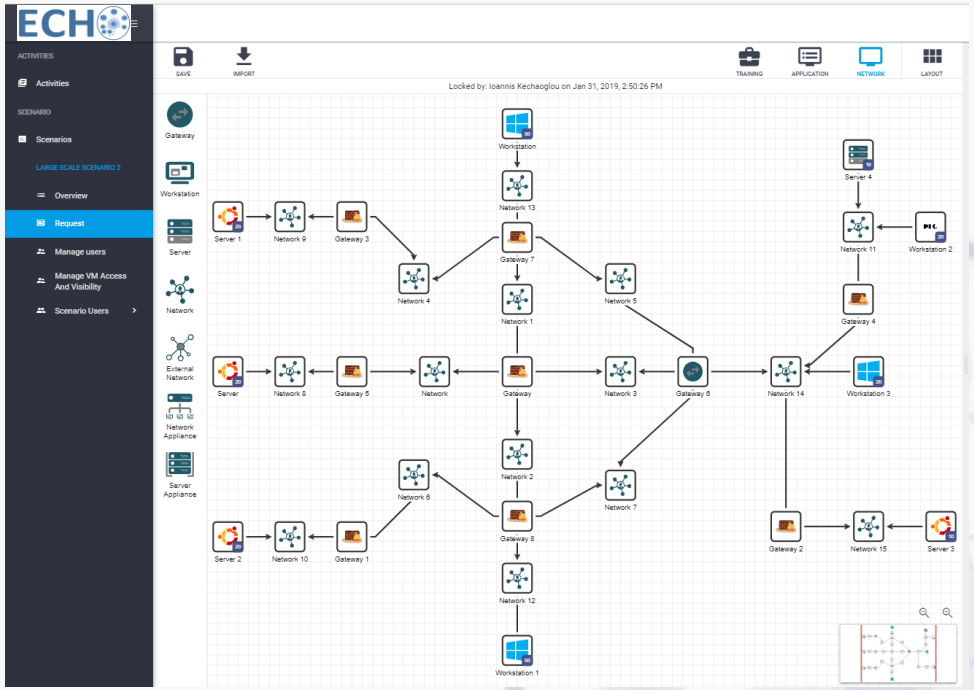


E-FCR concept



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

Critical Sectors EC-JRC taxonomy

Audiovisual and media	Defence	Digital infrastructure	Energy	Financial
Government and public authorities	Health	Maritime	Nuclear	Public safety
Tourism	Transportation	Smart ecosystems	Space	Supply chain

Demonstration cases for validation

- Sector demonstration cases
  - Scenarios are subject to clarification and amendment based on the results of the project, in particular the results of the sector and inter-sector analysis to be conducted using the E-MSAF.
  - Technologies will be demonstrated from the technology roadmaps in the demonstrations.
  - Importance of inter-sector dependencies.
- Technology demonstration cases
  - E-EWS
  - E-FCR

Demonstration cases for validation

- **Health sector**
  - ICT becoming more and more pervasive in health care
    - Computerized systems for automation of diagnostic and collection of patient data;
    - Sensors and medical devices with IP addresses connected to the Internet (IOT);
    - Cloud-based health information management systems;
    - Multidisciplinary teams interact with patient and share sensitive data also through personal devices.
  - Cybersecurity lagging behind when compared to other industries
    - Evidence that healthcare is rapidly growing target for hackers;
    - Sensitivity of personal data that could be destroyed or leaked to unauthorized third parties in the event of an intrusion.

Demonstration cases for validation

- **Marine sector**
  - Already very digitized
  - Major economic sector of strategic importance
  - Digital systems on vessels can be divided in two main categories:
    - Information Technology networks (IT), the hardware and software dedicated to manage and to exchange information; it belongs to IT networks.
    - Operational Technology networks (OT), the hardware and software dedicated to detecting or causing changes in physical processes through Industrial Control Systems.
  - Both networks highly integrated, raising specific challenges, cfr. the cyber kill chain for ICS
  - Risk Management must encompasses all digital systems on board, resulting in specific technical cyber security controls as well as procedural controls

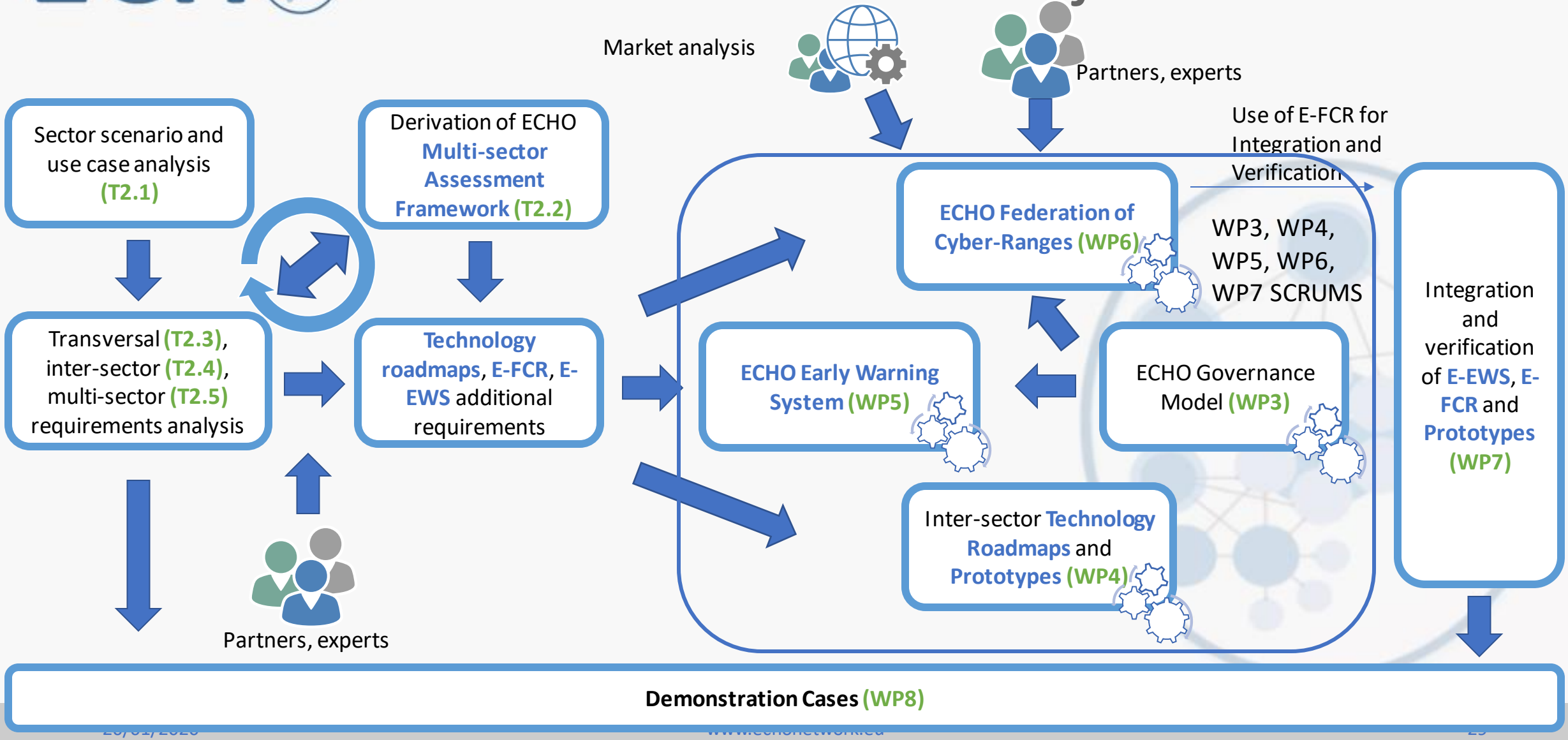
Demonstration cases for validation

- **Energy sector**
  - Security of critical infrastructure is essential for the safety and security of citizens and the industrial capacity across the EU
  - Some use cases to be considered:
    - Attacks to the command and control systems of the critical infrastructure (unavailability, loss of serviceability, subversion of a C2 center)
    - Attacks to SCADA equipment/devices of the critical Infrastructure

Demonstration cases for validation

- **Defence sector**
  - Complex high-tech environment will large amount of cyber-physical systems
  - Reducing budgets
  - Lot of legacy equipment
  - Mobile systems with disadvantaged tactical networks
  - High probability: weapon systems are actively targeted from the cradle to the grave
  - High impact: loss of life, international conflict escalation, …

Project Structure



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, training
  - 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..), potentially at EU level
  - 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**

The first 2 years

- ECHO schedule for the first 2 years is quite tight
  - **E-EWS** and **E-FCR TRL 6** prototypes to be developed for **mid 2021 - ongoing**
  - Governance Models (and related transition from the current model) for the network will be ready for **mid 2021**
  - Preliminary models for **sustainability** of the network, the E-EWS and the E-FCR
  - Goal is to immediately deploy E-EWS (**already operational**) and E-FCR and start using them within the ECHO **enlarged partners** (beneficiaries + stakeholders) – **new tenants** for the E-EWS and **new cyber ranges** for the E-FCR (many with **RHEA CITEF Technology**!)
  - Training packages will be ready for **mid 2021** and in delivery, leveraging on E-EWS and E-FCR prototypes
  - **Healthcare**, **Maritime**, **Energy** sectors demonstrations in development (including dependencies with space and water sectors, likely)
  - Other 2 technology innovations (at least) from the technology roadmaps will be in development

Engagement Opportunities

- ECHO is interested on enlarging the number of partners, when newcomers can bring an added value to the team
- Parties interested in ECHO will be mapped into the following categories:
  - Stakeholders
  - Potential new partners (R&D and Operational phases)
    - N.B. New partners are considered a subset of stakeholders.
  - Beneficiaries (of grant agreement)
    - N.B. Beneficiaries are currently fixed.
  - Project Advisory Committee Members
    - 15 members (5 identified)
    - Advise on strategic global trends, best and common practice, legal and ethical aspects, concept assessment, scenario definition and prioritization, analysis of operational environments, and test and validation;
    - Help strengthen the ECHO environment, leveraging on their network & experience.

Title	Definition
Stakeholders	Stakeholders are people or organisations who have an interest in the project and can either affect or be affected by the results. Such as users of the services, members of management boards, steering committees, regulatory or policy groups/bodies, lobby groups and suppliers etc.
Partners	Partners are stakeholders who wish to become more active in the project and become contracted parties, offering either funding, technical support or other services in exchange for collaborating in R&D activities.
Beneficiaries	Partners who wish to become active parties within the Consortium requiring a Grant Agreement amendment. Participate in R&D activities within scope of ECHO.

Social Media

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

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