ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

The gamification of Cyber Security

Andrea Guarino

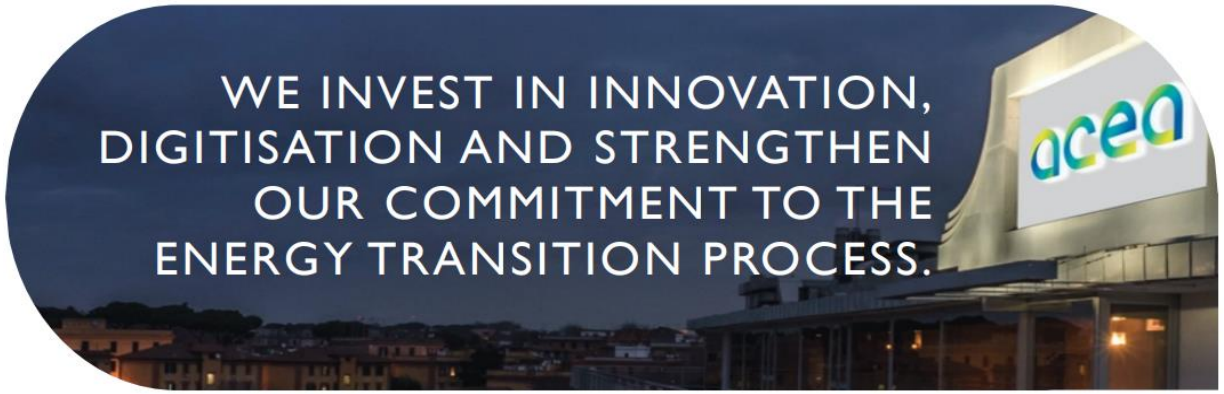
Resp. Security Awareness & Training
Cyber Security - Technology & Solutions
Acea SpA

Apulia CyberSecurity Forum 2021 – 2a edizione

November 11, 2021

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

A LEADING INTEGRATED MULTIUTILITY IN THE ITALIAN MARKET



WHICH INVESTS IN SUSTAINABILITY, A PRIMARY FACTOR GUIDING THE GROUP'S BUSINESS STRATEGIES, COMBINING ECONOMIC GROWTH AND VALUE CREATION.

Leader in the integrated water sector and one of the leading operators in the electricity distribution, energy and environment sectors, it is a company that puts its business and expertise at the service of the territory and its citizens. The Group's industrial vocation also passes through the strategy of sustainable growth and innovation, cross-cutting development leverage applied to every business activity.

Cybersecurity Challenges for the EU

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

1

Retain and develop essential capacities to secure its digital economy, infrastructures, society, and democracy

2

Better **align cybersecurity research, competences and investments**

3

Step up investment in **technological advancements** to make EU's **digital single market more cybersecure** and overcome fragmentation of research

4

Master **relevant cybersecurity technologies** from secure components to trustworthy interconnected IoT ecosystems and to self-healing software

5

Support industries and equip them with latest technologies and skills to **develop innovative security products and services** and protect their vital assets against cyberattacks

6

Contribute to the objective of European **strategic autonomy**

Let's ask to an expert:

MR. ROBOT

« This is the world we live in. People relying on each other's mistakes to manipulate one another, use one another, even relate to one another. A warm, messy circle of humanity. »

« People are all just people, right? When it gets down to it, everyone's the same. They love something. They want something. They fear something. Specifics help, but specifics don't change the way that everyone is vulnerable. It just changes the way that we access those vulnerabilities. »

Cybersecurity Challenges for the EU

This Cybersecurity challenge is critical: we simply don't have enough security experts

2

Better **align cybersecurity research, competences and investments**

- We lack cybersecurity professionals, but we have plenty of untrained and unaware users;
- "Human Factor" (mostly, misbehaving done by unprepared users) is the main cause of security breaches, data leaks, phishing and cyber-attack incidents;
- Humans have hard-wired exploitable vulnerabilities in their Mind OS;
- Humans tend to avoid or forget boring, repetitive trainings;
- Humans like to PLAY GAMES, especially if they can do it against other humans or competent AI;

If we want to engage everyone (both users and professionals), we must gamify their User Experience and their training / awareness courses.

Some definitions of “game”

“[...] a word like “game” points to a somewhat diffuse “system” of prototype frames, among which some frame-shifts are easy, but others involve more strain” (Marvin Minsky, American cognitive and computer scientist)

“A structured experience with rules and goals that is fun.” (Amy Jo Kim, GameThinking coach and UX designer)

“The voluntary attempt to overcome unnecessary obstacles” (Bernard Suits, Distinguished Emeritus Professor of Philosophy)

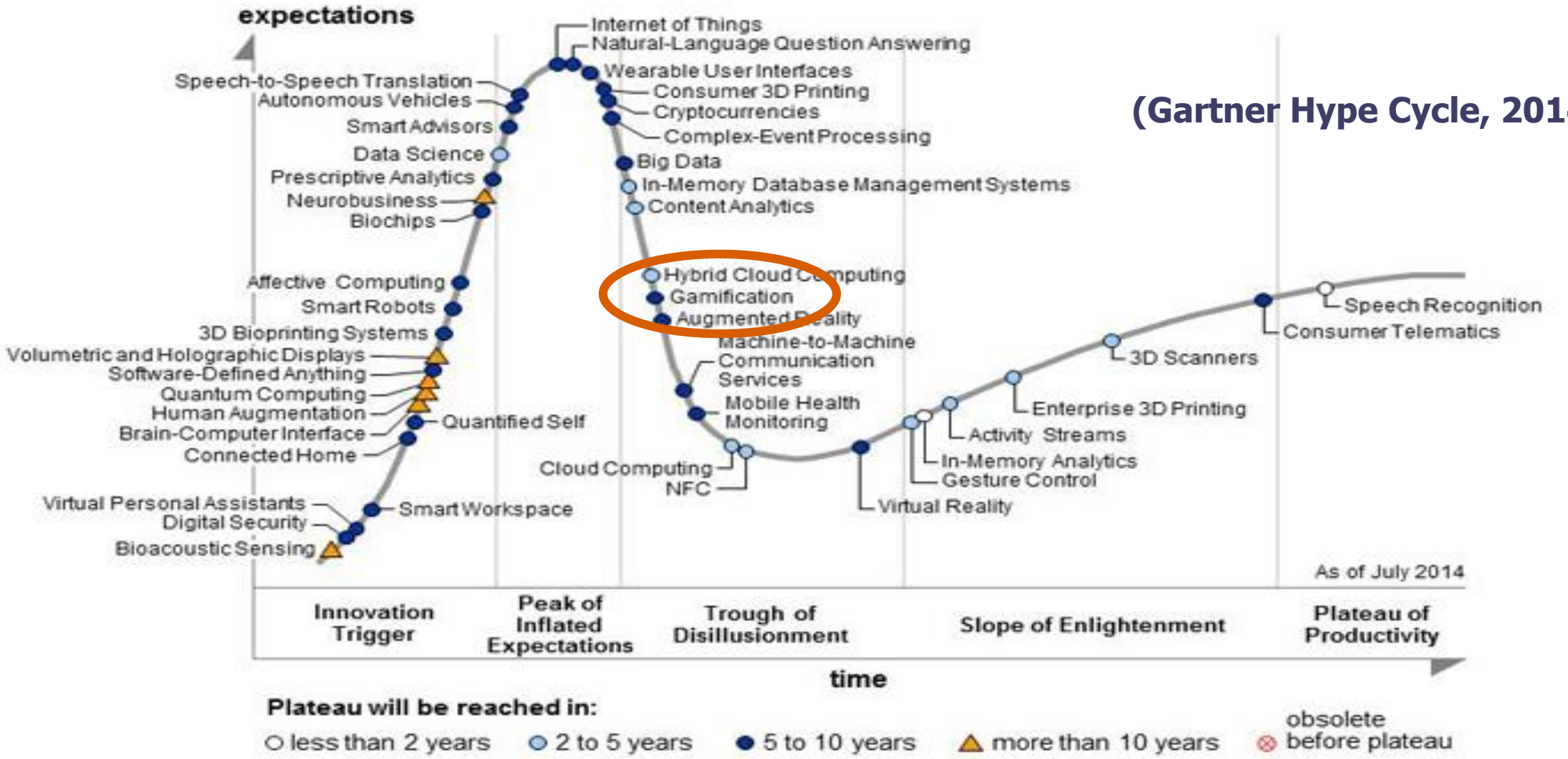
“A series of meaningful choices” (Sid Meier, author of the videogames “Pirates!” and “Civilization”)

“A game is a problem-solving activity, approached with a playful attitude.” (Jesse Schell, Distinguished Professor of the Practice of Entertainment Technology, Videogame Designer)

“A game is a system in which players engage in an artificial conflict, defined by rules, that results in a quantifiable outcome.” (Eric Zimmerman and Katie Salen, game designers / game design theorists)

“Play” becomes a “game” when you impose system-based rules and set explicit goals

What is “Gamification”?



(Gartner Hype Cycle, 2014)

What is “Gamification”?

“Gamification is the use of game mechanics and experience design to digitally engage and motivate people to achieve their goals. It is important to distinguish gamification from video games and loyalty programs, as gamification uses techniques from behavioral science to “nudge” people into achieving their goals.”

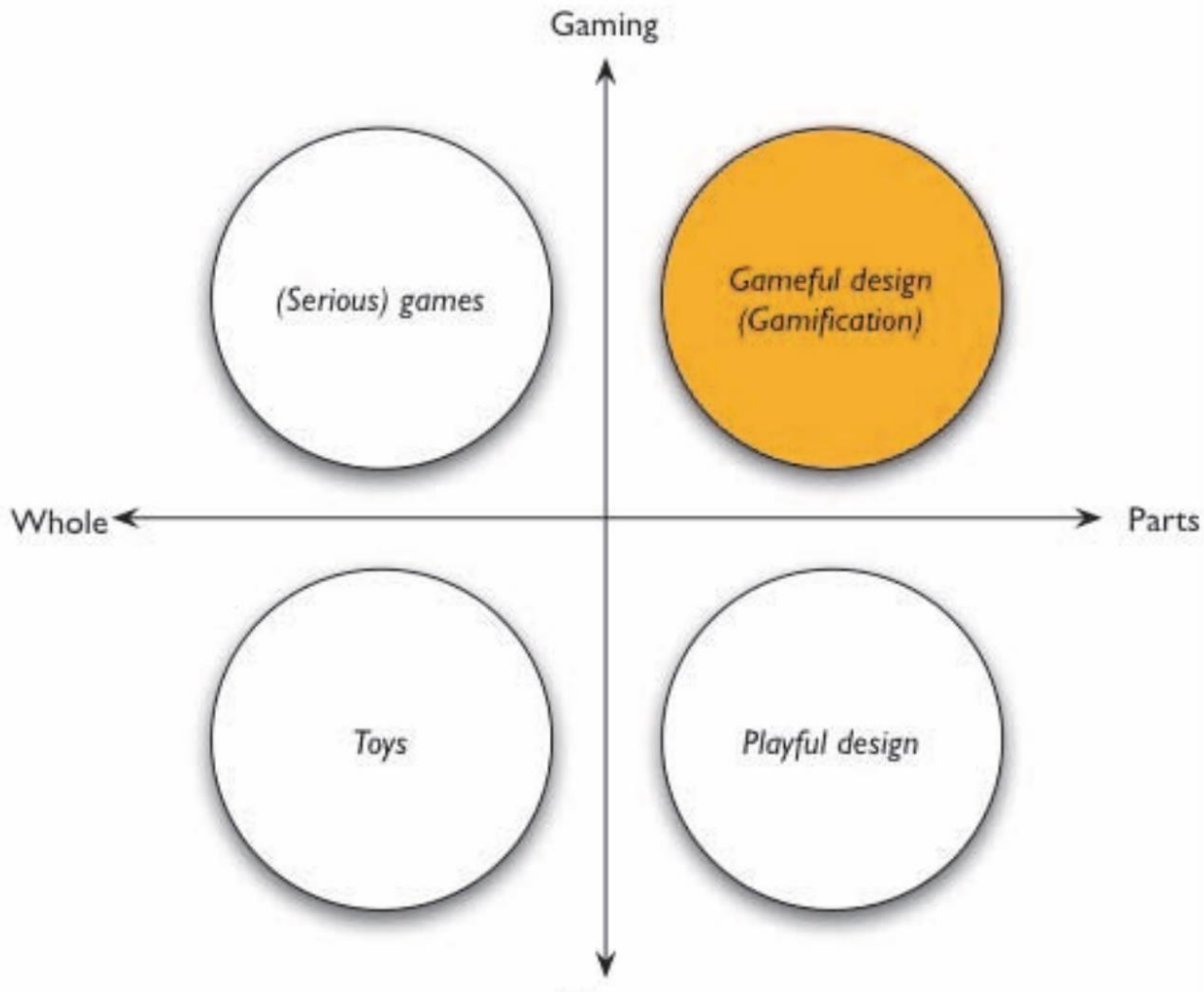
(Gartner definition)

“Gamification” is a serious matter, but not equal to “serious games”

“Gamification” refers to:

- the **use** (rather than the extension) **of**
- **design** (rather than game-based technology or other game related practices)
- **elements** (rather than full-fledged games)
- **characteristic for games** (rather than play or playfulness)
- **in non-game contexts** (regardless of specific usage intentions, contexts, or media of implementation).

[Deterding, Sebastian & Dixon, Dan & Khaled, Rilla & Nacke, Lennart. (2011). From Game Design Elements to Gamefulness: Defining Gamification]



We need both to cover all the challenges

"Gamification" programs typically enable the use of rosters, prizes, experience points, badges and team competitions, without changing in a significant way the underlying systems. Good choice for general audience to upgrade UX.

"Serious games" are immersive, complex and exhaustive. They are difficult and costly to realize. Tabletop card-based games are well suited for small groups of managers and executives, particularly for breach and attack simulations.

Although "Serious Games" are used for training purposes, they still maintain the major advantage of being funny and interactive. They enable people to develop skills and thoughts through a fun and interactive way and they provide the needed adaptability and flexibility that a game requires to keep participants engaged.

ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD innovAtion

Cyber Security for Europe

SPARTA

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Partners

Project Coordination:
Royal Military Academy of Belgium (Wim Mees)

Project Management:
RHEA System S.A. (Matteo Merialdo)

- 16 Millions budget
- 4 years (started Feb 2019)
- 30+7 partners
- 15 new partner engagements
- 13 existing competence centres
- 18 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Cybersecurity Challenges for the EU

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

- Lack of effective means **to assess multi-sector technology requirements** across security disciplines
- Lack of effective means to **assess dependencies between different industrial sectors**
- Lack of **realistic simulation environments** for technology research and development, or efficient security test and certification

- Lack of an **up-to-date cyberskills framework** as a foundation for cybersecurity education and training
- Lack of effective **means to share knowledge and situational awareness** in a secure way with trusted partners
- These gaps **are particularly relevant for EU**

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ECHO Main Objectives

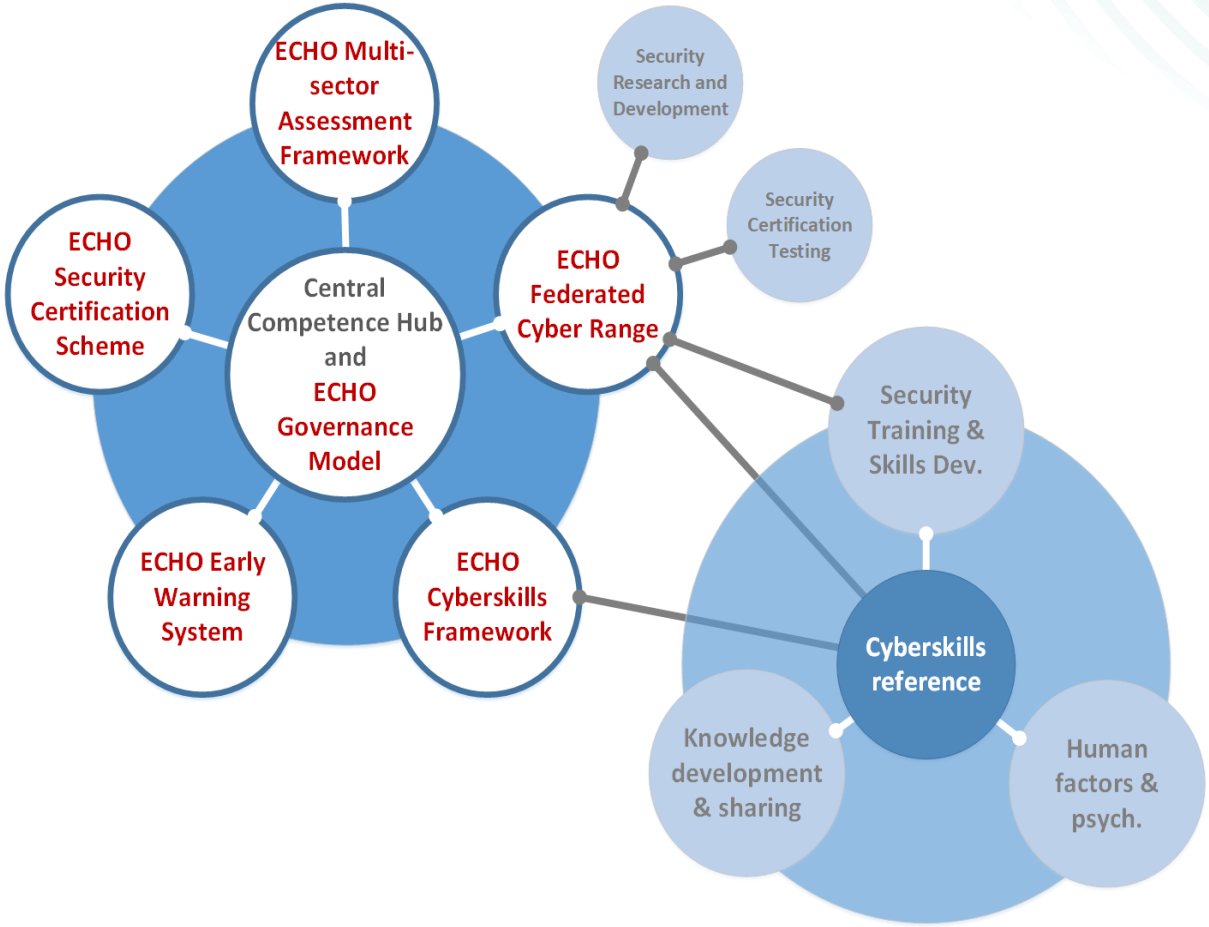
The network of cyber research and competence centres, with a central competence hub has the following goals:

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

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ECHO Cyberskills and Training Curricula

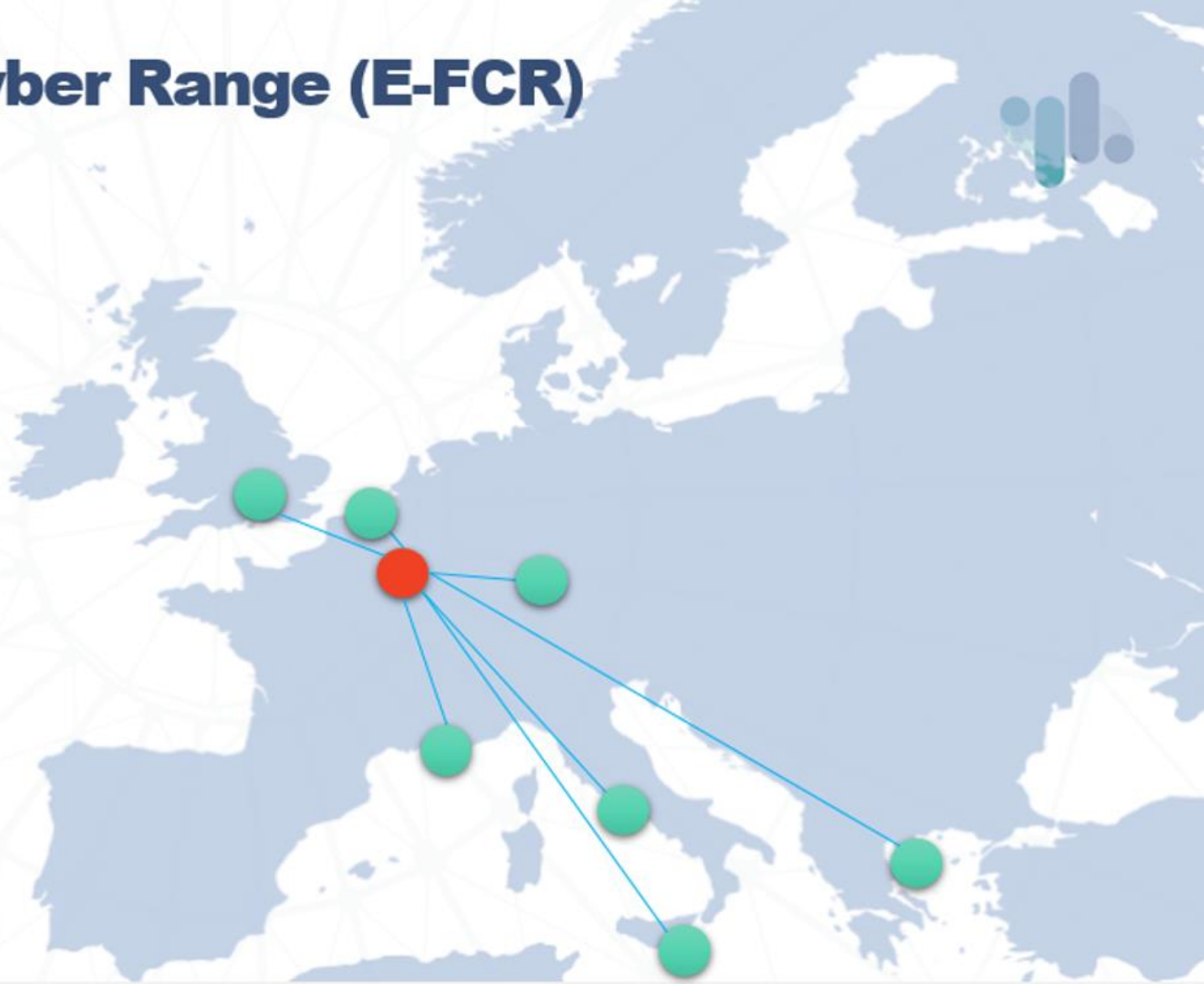


ECHO Cyberskills framework

- 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 Federated Cyber Range (E-FCR)

- We will need to deploy E-FCR Agents in the ECHO cyber ranges
- This will help also testing and validation of E-FCR

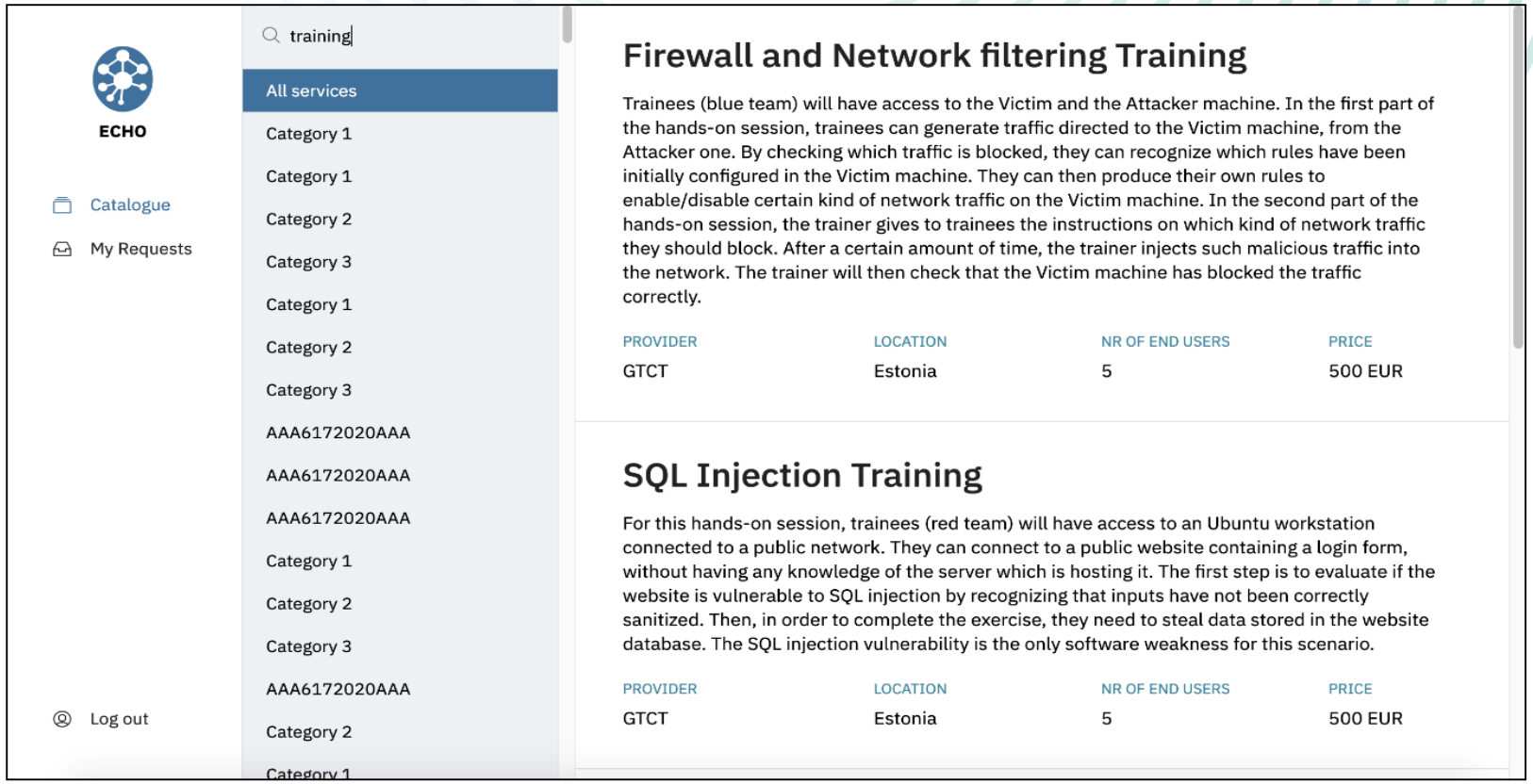


The ECHO Federated Cyber Range (E-FCR)

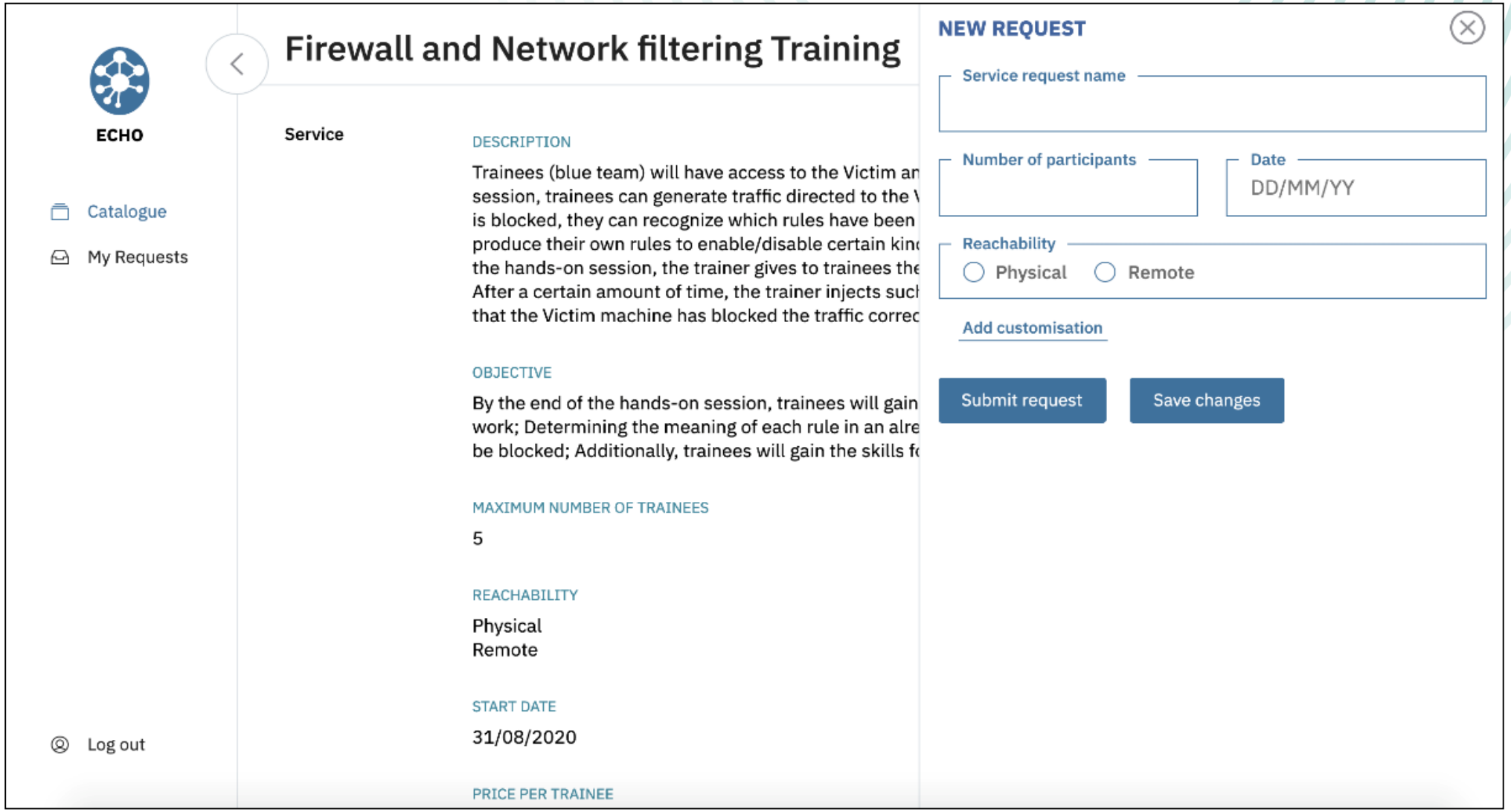
Concepts

Customers will have access to

- **Capacity and Capability Maps** of the federated ranges
- **Service Designer** -> collect User Requirements via a **Scenario Description Language** and its GUI
- **Marketplace** (Content Providers can upload contents/scenarios for a wider market)
- **Automated VPN connection** between ranges to provide technical federation

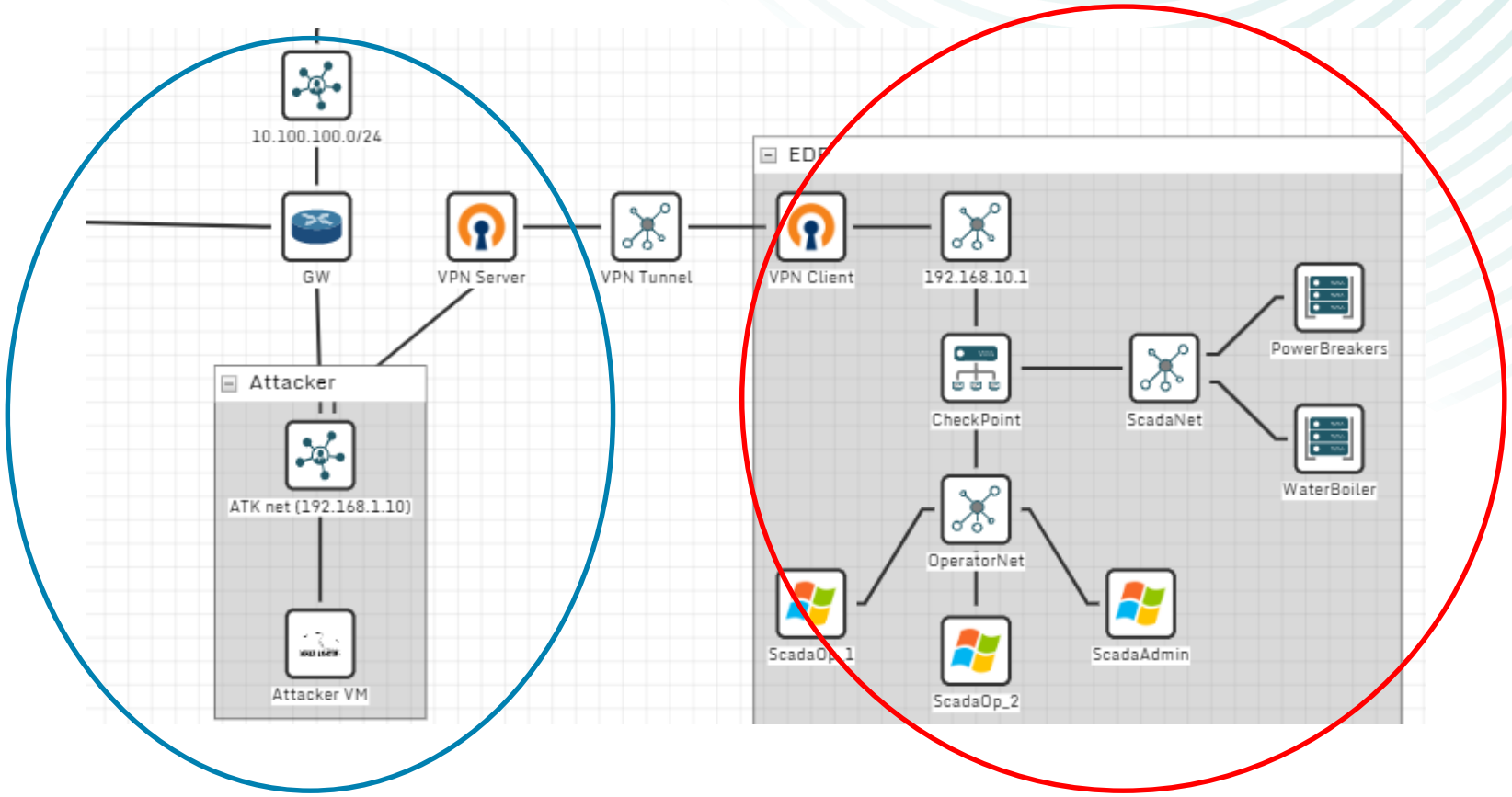


E-FCR Marketplace



Interconnection between Cyber Ranges

- The VPN Client/Server approach works perfectly, with a few limitations we consider negligible
- Tested with multiple CRs on **complex scenarios**



CYBER RANGE 1

CYBER RANGE 2

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**

Demonstration cases for validation

Energy Sector

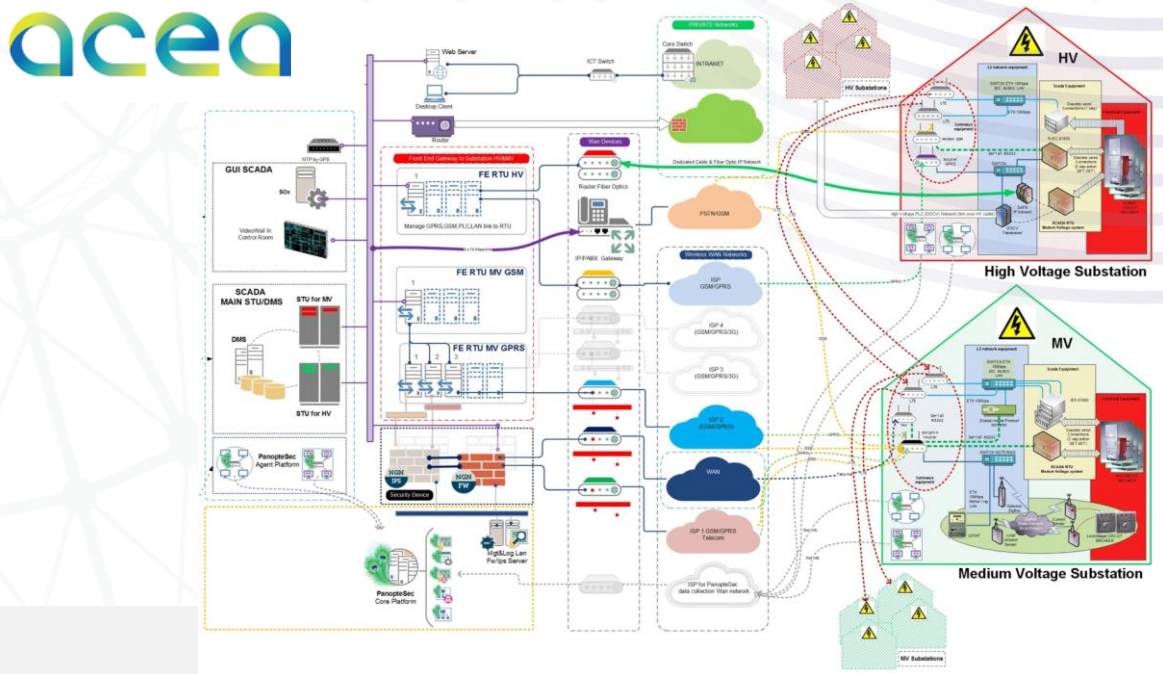
The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

The energy sector faces increasing and more sophisticated cyber threats affecting both the IT and OT side

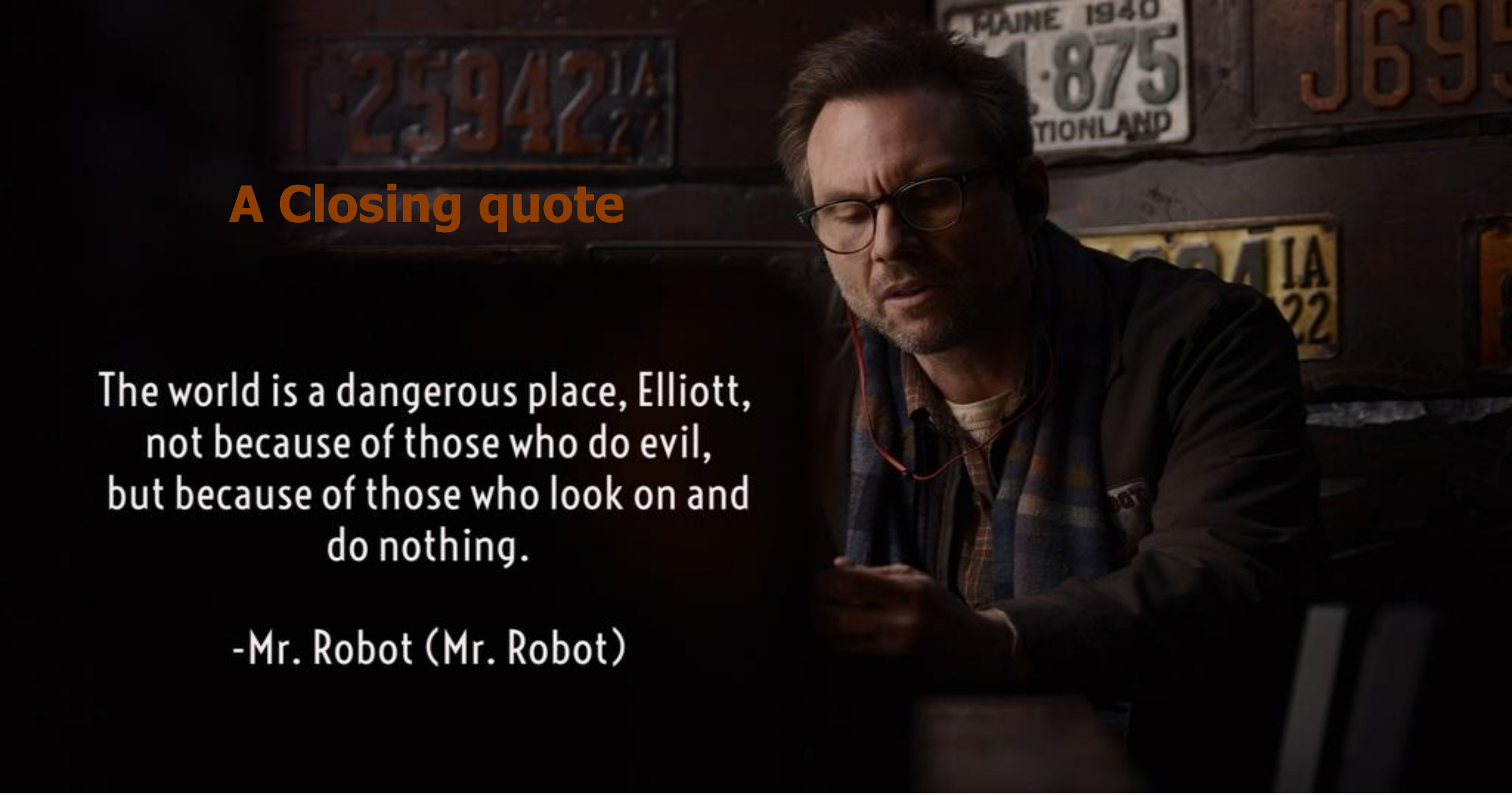
Some use cases to be implemented

- Attacks against the command-and-control systems of the energy provider
- Attacks to SCADA equipment/devices of the energy provider

We are creating a sector-specific cyber range emulating a C&C Centre to support the Demonstration Cases



A Closing quote



ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

info@echonetwork.eu

www.echonetwork.eu

https://twitter.com/**ECHOcybersec**

https://www.facebook.com/**echonetworkeurope/**

https://www.linkedin.com/in/**echo-cybersecurity**

https://www.youtube.com/channel/**UCDQBXrQhoLJ2lnf38x1X6Uw**

Andrea Guarino (Andrea.Guarino@aceaspa.it)

www.gruppo.acea.it