FORESIGHT

Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments

Christos Iliou

19 June 2019

Multimedia Knowledge and Social Media Analytics Lab
Information Technologies Institute
Centre for Research and Technology Hellas (CERTH)

Turkey in Horizon 2020 Phase II, International Study Visit to CERTH
Thessaloniki, Greece

FORESIGHT Overview

1. General Information
2. Consortium
3. FORESIGHT for Digital Security
4. Concept
5. Pilot Use Cases (PUCs)
6. Work Packages
7. Innovation
8. Exploitation & Dissemination
9. Impact & Benefits

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

General Information

FORESIGHT: General Information

Project Coordinator: European Dynamics S.A. (ED), Luxembourg

Start Date: 01/09/2019

Duration: 36 months

Type of Action: Innovation Action (IA)

Overall budget: € 7,342,523.75

Consortium: 21 partners (5 research, 5 academic, 10 industry, 1 government agency)

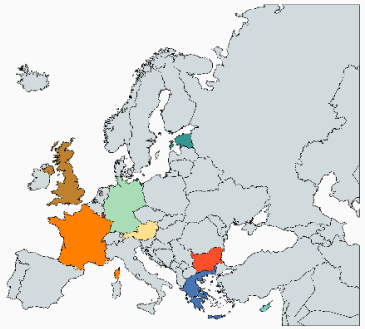


Figure 1: FORESIGHT partners

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Consortium

FORESIGHT: Consortium

Industry

- ED
- CRI
- INC
- CCS
- CYB
- AIA
- THALES
- IEIT
- ESO
- CEZ

Research

- KEMEA
- CERTH
- CENTRIC
- M&S
- BDI

Academic

- UOP
- UAD
- CSCAN
- OUC
- EN

Government Agency

- CERT-BG

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

FORESIGHT for Digital Security

FORESIGHT for Digital Security

The FORESIGHT project aims to develop a **federated cyber-range solution** in order to **enhance the preparedness of cyber-security professionals at all levels** by delivering a **realistic training and simulation platform** that brings together unique cyber-security aspects from the aviation, power grid and naval ecosystems.

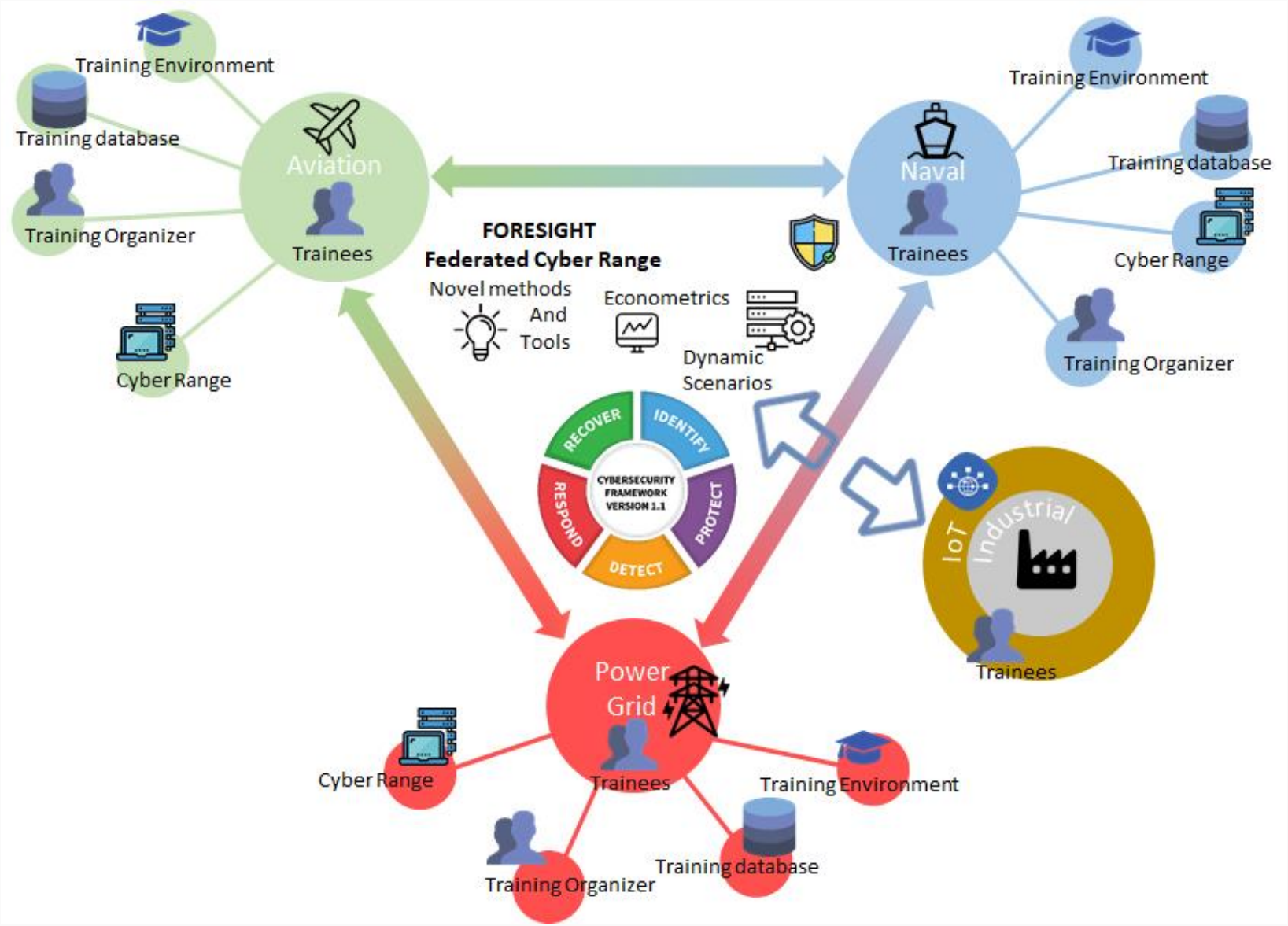
FORESIGHT main objectives:

- Federation: (current future) cyberranges and training environments, cross-domain scenarios
- Dynamic scenarios based on identified/forecast threats using online sources (Surface/Dark Web)
- Advanced, constantly updated risk analysis and econometric models
- Innovative training curricula (linked to professional certification programs)
- Enhance the preparedness of cyber-security professionals at all levels

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Concept

FORESIGHT: Concept



This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Pilot Use Cases (PUCs)

FORESIGHT Pilot Use Cases (PUCs)

PUCs

1. **Aviation**: Simulation of network and the critical IT services (hardware components and virtual machines)
2. **Naval**: simulate different functionalities of a boat.
3. **Power grid**: simulate the office and grid infrastructure.
4. **Hybrid domain**: includes physical and virtualised machines, industrial IoT devices
    - SCADA controlled general, physical PLCs, etc.

Scenarios

- Detection and Prevention of Cyber Attacks
- Network monitoring and management
- Cyber-attack countermeasures and automation of cyber-attack responses
- Situational awareness and control
- Analysis of economic impact of cyber incidents
- Teamwork: delegation, dividing and assigning roles, leadership

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Work Packages

FORESIGHT Work Packages

No	Title	Lead	Person months	Start month	End month
1	Project management and coordination	ED	21	1	36
2	FORSIGHT Architecture and user requirements	AU	67	1	30
3	Ethical, legal and societal aspects	CRI	34	1	36
4	FORESIGHT training methodology	CSCAN	110	1	36
5	Cyber-security risks and econometrics	INCITES	54	1	24
6	Training program #1: Aviation	CCS	58	2	24
7	Training program #2: Power Grid	CYB	89	2	24
8	Training program #3: Naval	EN	48	2	24
9	FORESIGHT toolkit development	UOP	96	8	24
10	FORESIGHT platform federation and testing	OUC	82	6	35
11	Pilot implementation and evaluation	KEMEA	97	1	36
12	Impact sustainability	M&S	68	1	36

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Innovation

FORESIGHT Innovation I

WP4: FORESIGHT training methodology

- Understanding training needs
- Identify training and learning objectives
- Innovative Curricula for training and evaluation
- Certification program

WP5: Cyber-security economic models

- Threat forecasting
- Econometric models for economic assessment of cyber-attack
- Risk analysis and assessment

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

FORESIGHT Innovation II

WP6,7,8: Training programs (Aviation, Power grid, Naval)

- Infrastructure modeling and simulation
- Training use cases
- Forensics evidence collection and analysis
- Develop detection methods for cyber-attacks
- Optimise cyber-defence strategies

WP9: FORESIGHT toolkit development

- Gamification
- Cyber-security Visualisation module
- Training evaluation module
- Information gathering and sharing module
- Dynamic scenario generation module
- Middleware ecosystem/suite for collaboration

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Exploitation & Dissemination

FORESIGHT Exploitation & Dissemination

Exploitation

- Commercialise the tool itself or provide it as a service
- Provide consultancy services using the FORESIGHT experience
  - Risk assessment and the economic impact of cyber-attacks
- Target: European and National public authorities as well as private companies
- Patent innovative outcomes of the project

Dissemination

- FORESIGHT's Website and social media accounts
- Liaisons with relevant universities, national, European and global RD projects
- In house presentations to industrial partners and interested parties
- Public open days across Europe
- Scientific and academic communities: journals, conferences, cybersecurity scientific society meetings, Open Access documents

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Impact & Benefits

FORESIGHT Impact & Benefits

- Improve preparedness, detection and mitigation of cyberattacks
- Enhance cyber resilience of ICT systems
- Improve risk analysis models
  - Appropriate econometric models for cyber incidents
  - Improved knowledge on security investments
- Increase collaboration between Cyber Ranges and European-wide initiatives

This project has received funding from European Union's Horizon 2020 research and innovation program under grand agreement No. 833673

Thank you