SPIDER

a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

5G Trials Workshop

Prof. Christos Xenakis

14 October 2020

University of Piraeus, Greece

Project Information

- **SPIDER**: a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
- **Grant Agreement ID**: 833685
- **Topic**: SU-DS01-2018 Cybersecurity preparedness - cyber range, simulation and economics
- **Call**: H2020-SU-DS-2018
- **Funding Scheme**: IA - Innovation action
- **Funded under**: H2020-EU.3.7.4.
- **Overall Budget**: € 7 476 908.75
- **EU contribution**: € 5 746 595
- **Start Date**: 1 July 2019
- **End Date**: 30 June 2022

The Consortium

19 partners from **10 European** countries (high diversity)

- 5 x Large Industries

- 6 x Research Institutes and Universities

- 8 x SMEs

What is SPIDER?

- **SPIDER** is an innovative **Cyber Range as a Service** (CRaaS) platform that **extends** and **combines** the capabilities of **existing telecommunication testbeds** and **cyber ranges** into a unified facility for:

  - **testing** new security technologies

  - **training** modern cyber defenders in near real-world conditions, and

  - **supporting** organisations and relevant stakeholders in **making** optimal cybersecurity investment decisions

The Challenges

- The emergence of **5G architecture** raised **radical changes** in the **telco domain**

- The core architecture **introduces** a **completely new landscape** for both **operators** and application **developers**

- 5G incorporates **many advanced technologies** (e.g. SDN, NFV, Virtualization) each of which **exposes its own attack surface**

- The 'new operational landscape' contributes in the **increase of cyber attack surface**

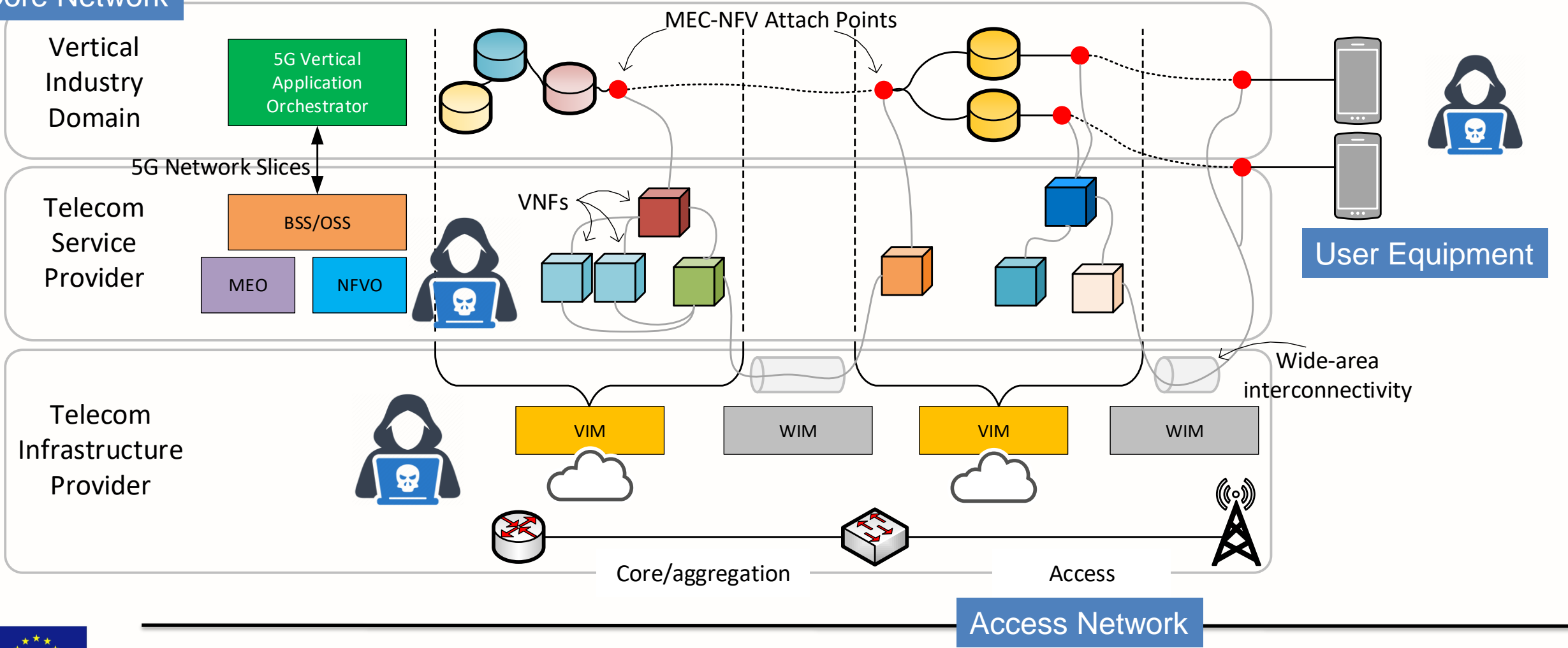- The **deficiency** in **cyber security experts**

The complexity of today's cybersecurity landscape emphasises the need for **highly competent experts** in **securing critical** multi-tenant and multi-service **environments**, such as 5G mobile networks.

5G Threat Landscape

Goals / Objectives of SPIDER

- To **develop** a **Cyber Range as a Service platform** targeting the specifies of **5G infrastructure**

- To **realize** an engine capable of **modelling** and **emulating** network **services** and **applications** as well as **complex cyber-attacks**

- To **provide active learning strategies** towards increasing the **cybersecurity skills** and **awareness** of **modern cyber defenders**

- To **implement** capabilities for **tracking** the **trainee's activity**

- To **integrate cyber range-driven risk analysis** and **propose econometric modelling tools** capable to forecast the **economic impact of cyber risks**

The proposed solution – a novel Cyber-Range Platform

- the **5G virtualisation platform** for the **deployment** and **configuration** of the **network infrastructure** replicating the elements for physical networking, storage, servers and test equipment;
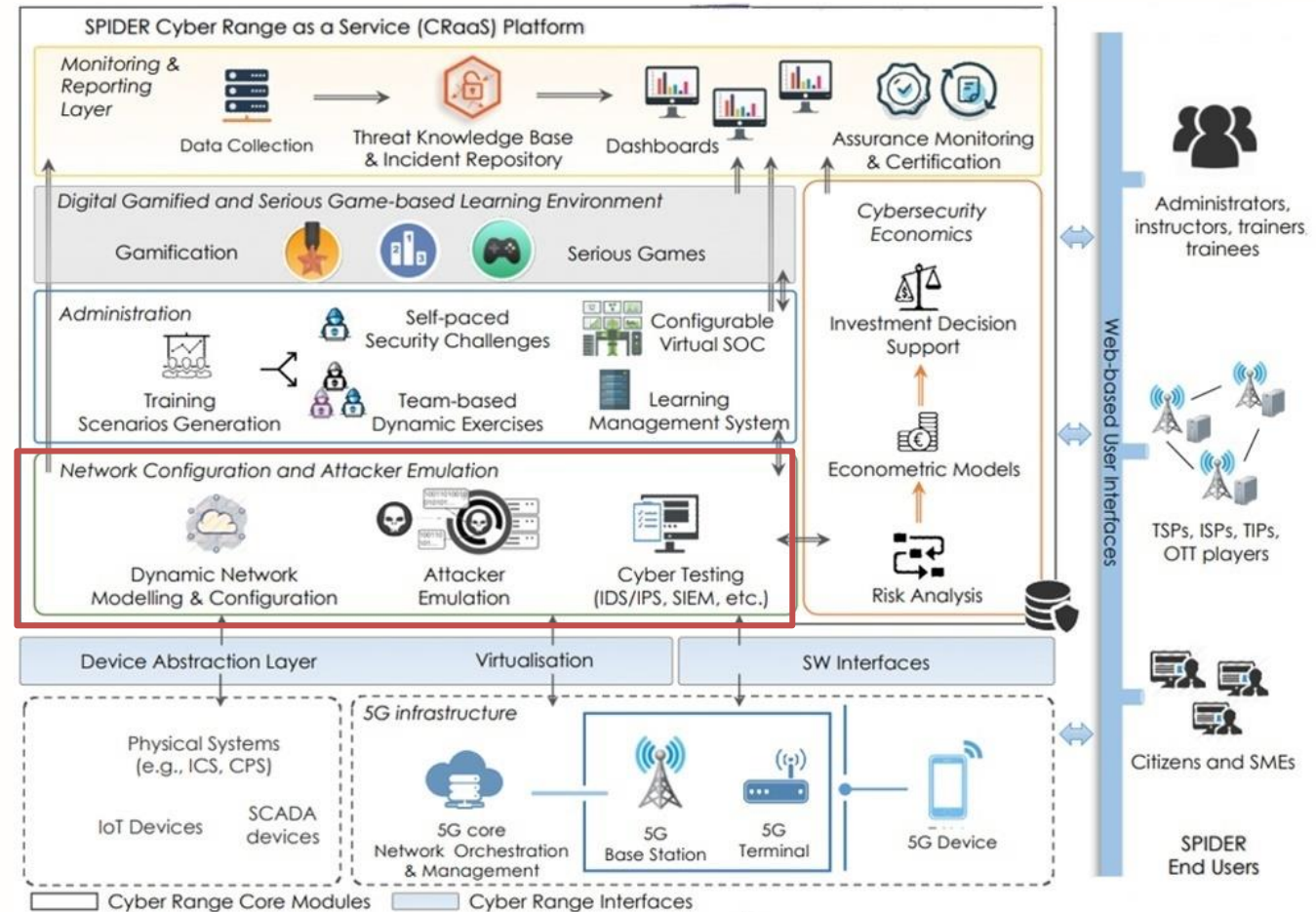
6 building blocks architecture
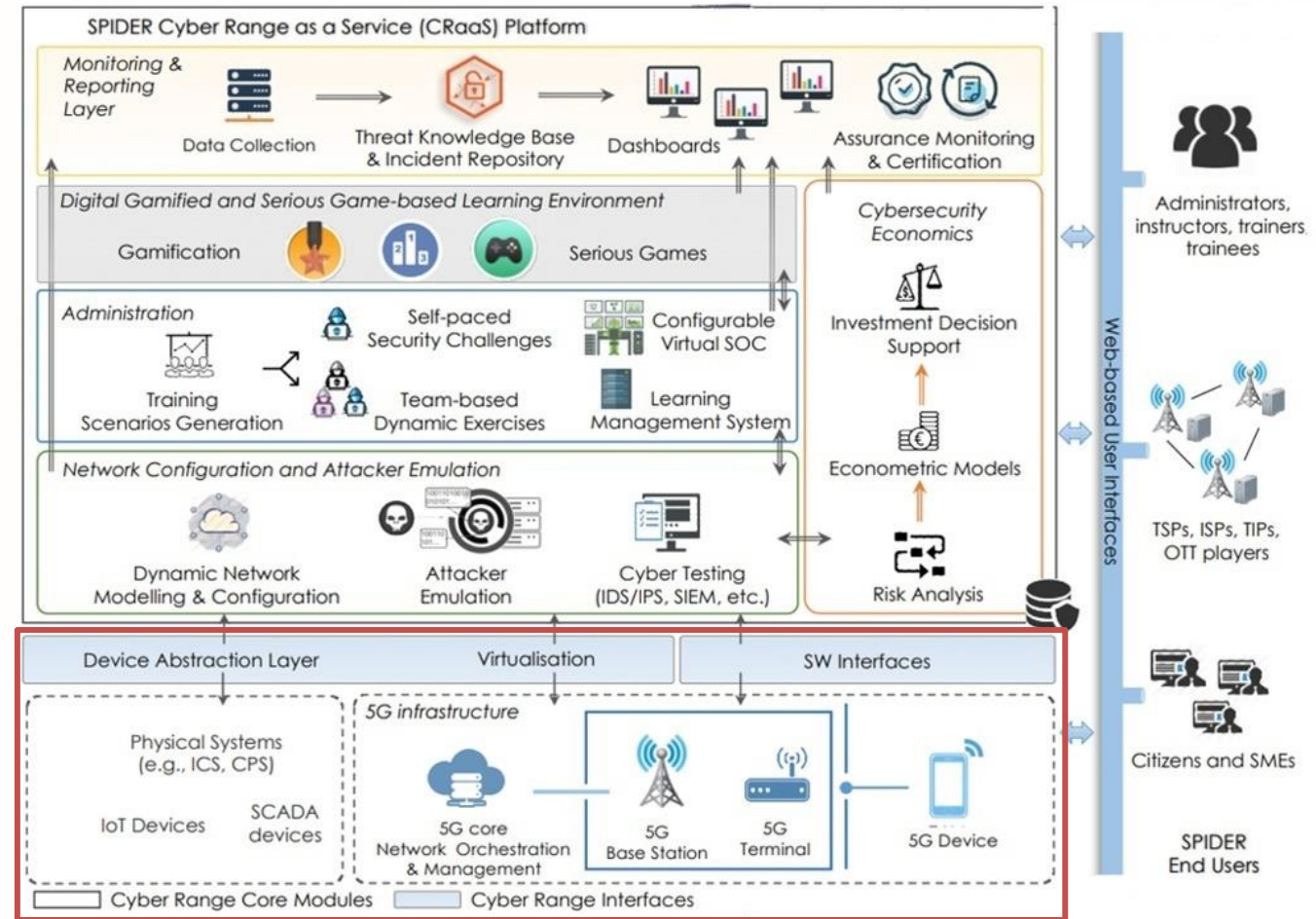
The proposed solution – a novel Cyber-Range Platform

- the **5G virtualisation platform** for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;

- the **network configuration and attacker emulation block**, equipped with an **AI/ML-based engine**, for **modelling** and **emulation** of **network services**, **applications** and **security mechanisms**;
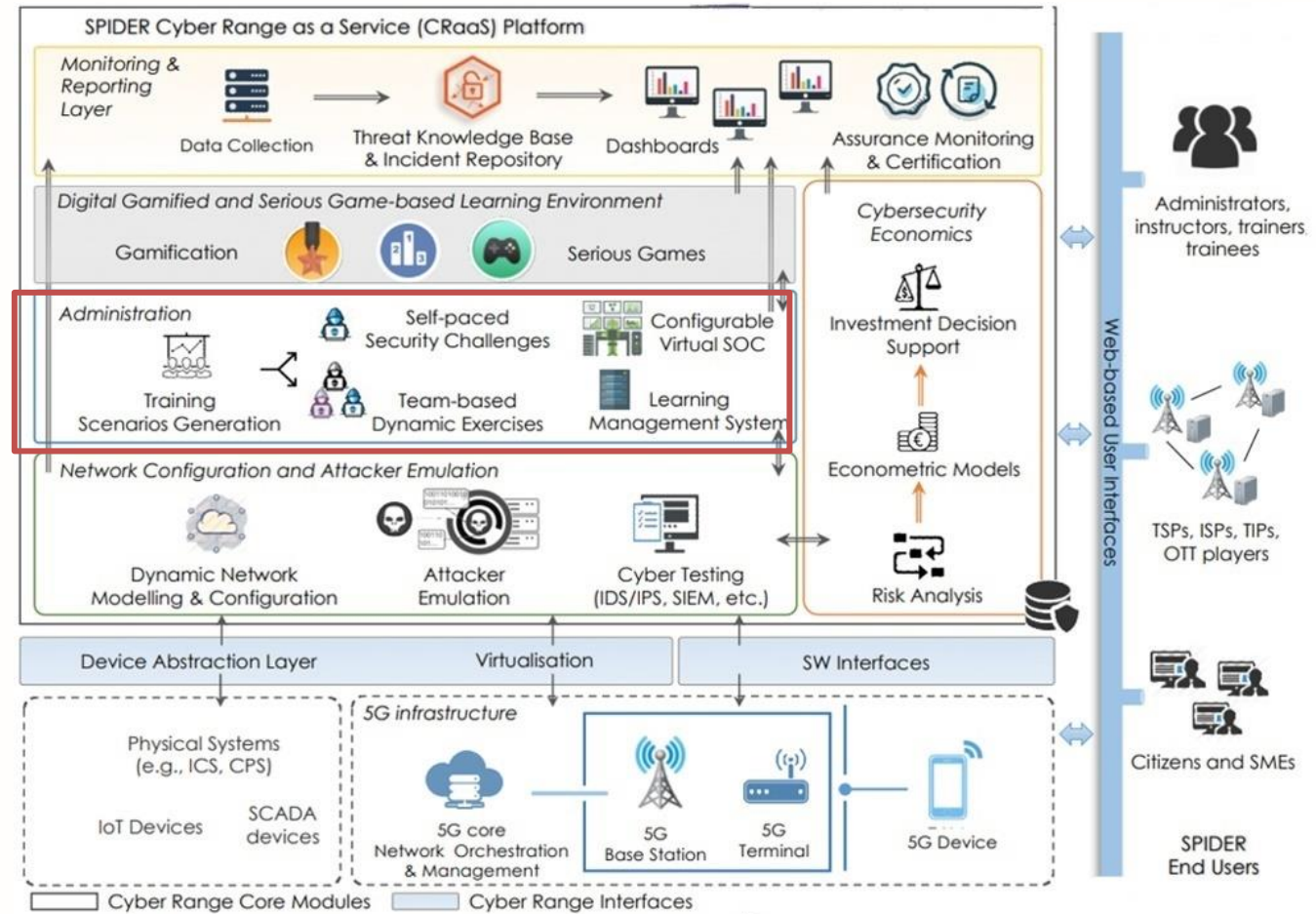
6 building blocks architecture

The proposed solution – a novel Cyber-Range Platform

- the **5G virtualisation platform** for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;

- the **network configuration and attacker emulation block**, equipped with an AI/ML-based engine, for modelling and emulation of network services, applications and security mechanisms;

- the **administration platform**, for the cyber range administrators to **configure** the **training scenarios**;
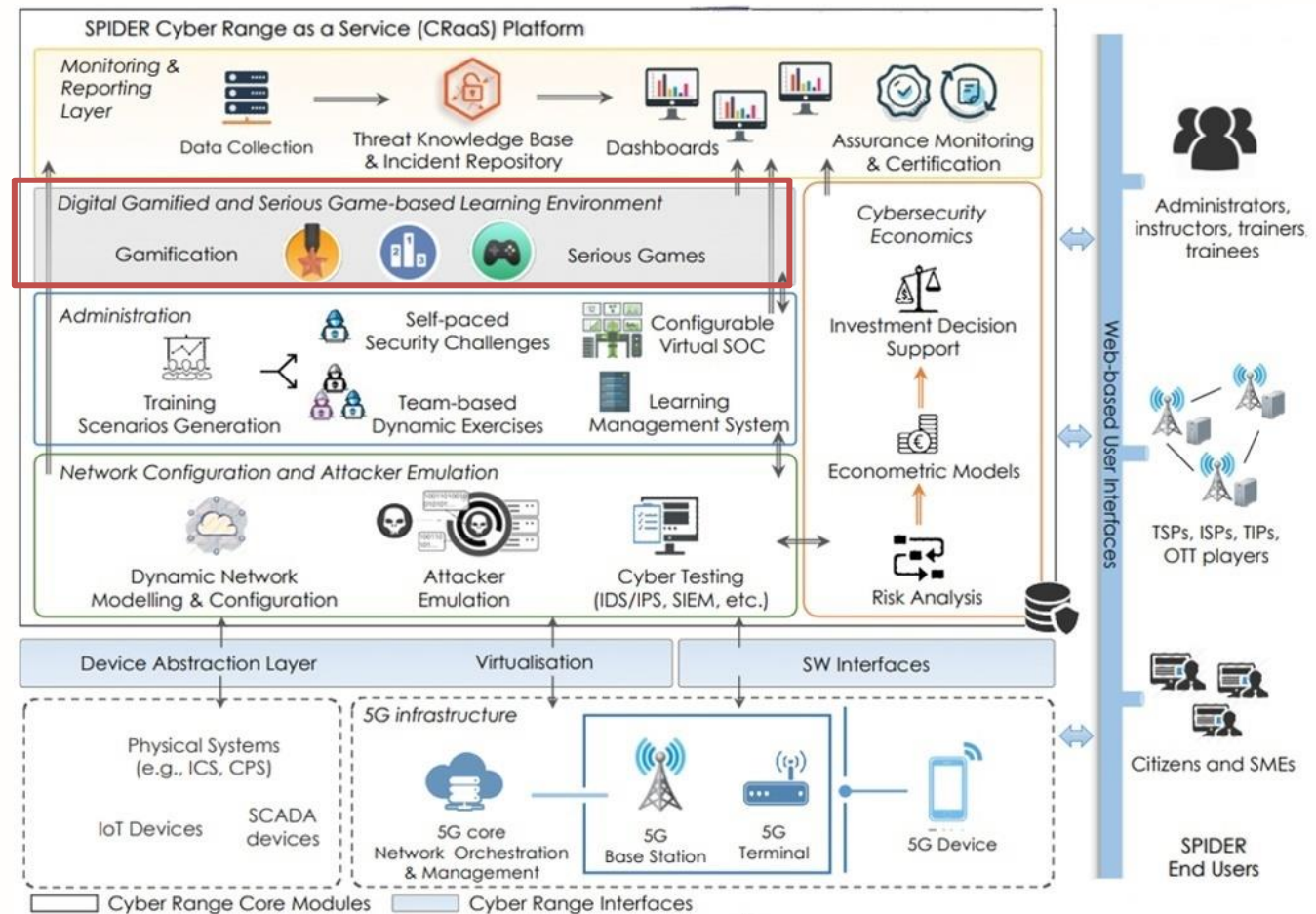
6 building blocks architecture

The proposed solution – a novel Cyber-Range Platform

- the **5G virtualisation platform** for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;

- the **network configuration and attacker emulation block**, equipped with an AI/ML-based engine, for modelling and emulation of network services, applications and security mechanisms;

- the **administration platform**, for the cyber range administrators to configure the training scenarios;

- the **digital gamified and serious game-based learning environment**, which is a simulation game framework leveraging on serious games and gamification solutions for training experts & non-expert users;
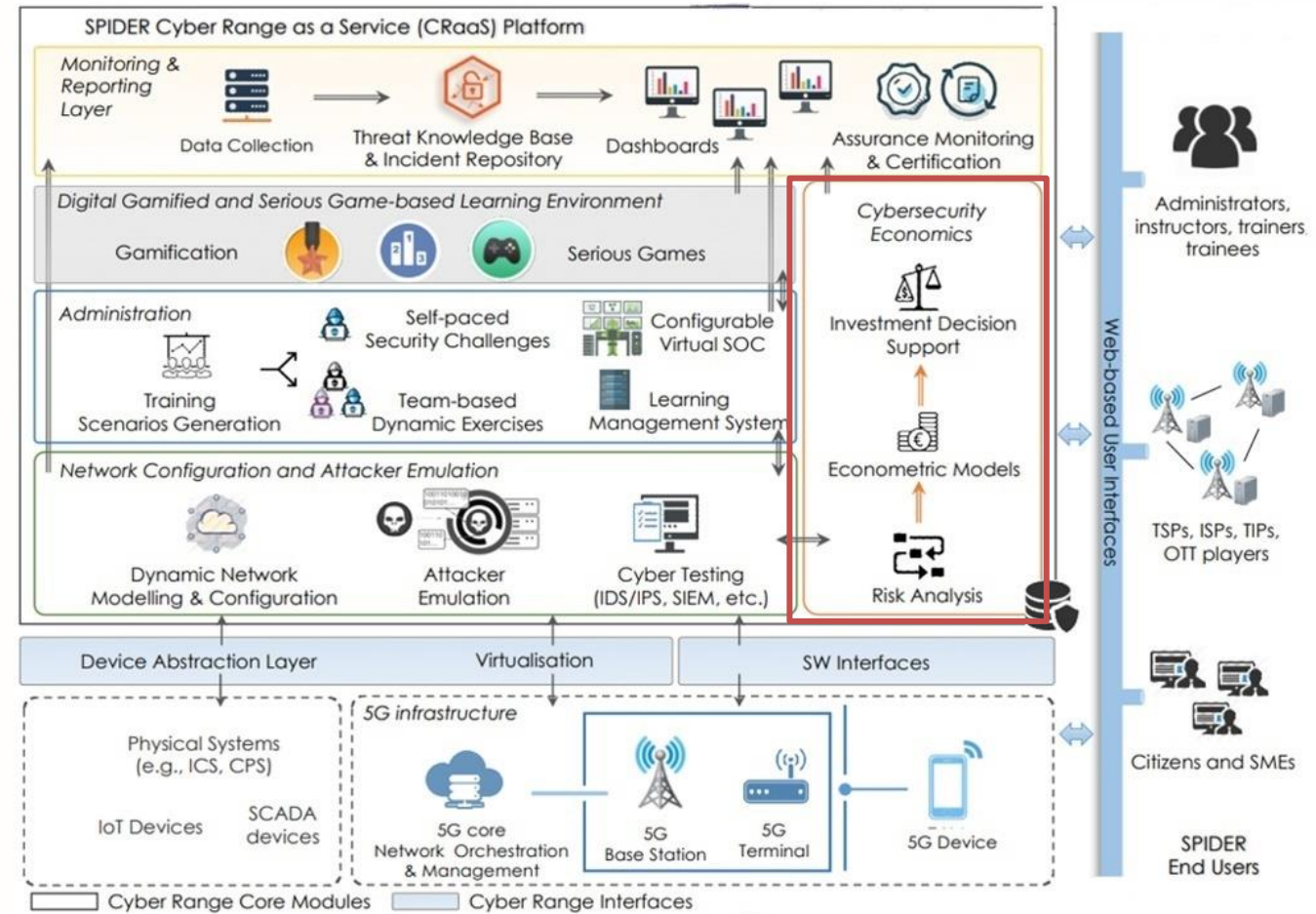
6 building blocks architecture

The proposed solution – a novel Cyber-Range Platform

- the **5G virtualisation platform** for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;

- the **network configuration and attacker emulation block**, equipped with an AI/ML-based engine, for modelling and emulation of network services, applications and security mechanisms;

- the **administration platform**, for the cyber range administrators to configure the training scenarios;

- the **digital gamified and serious game-based learning environment**, which is a simulation game framework leveraging on serious games and gamification solutions for training experts & non-expert users;

- the **risk analysis and cybersecurity economics block**, which **provides** the **forecast** for the **evolution of cyber-attacks** and their **associated economic impact**;
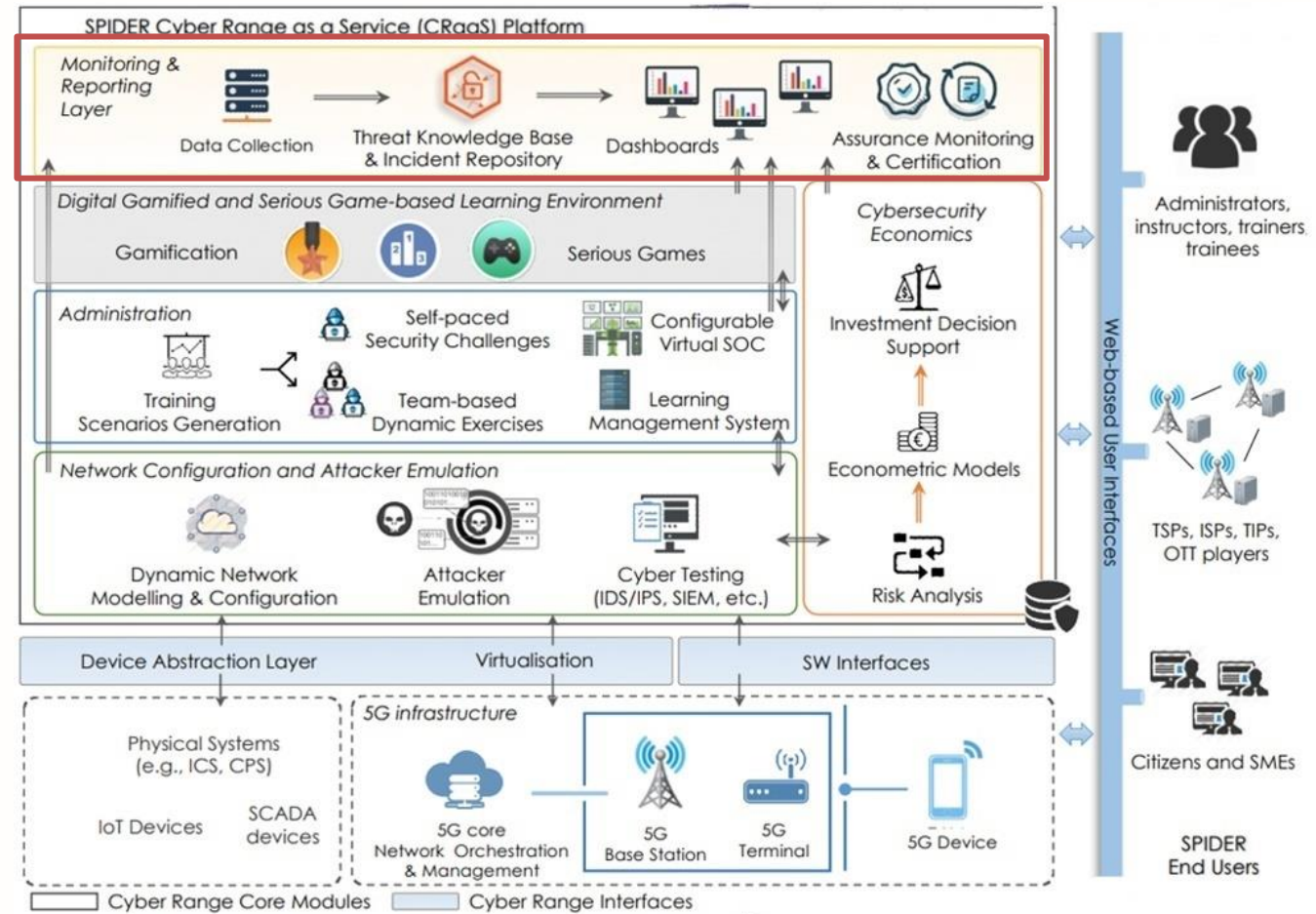
6 building blocks architecture

The proposed solution – a novel Cyber-Range Platform

- the **5G virtualisation platform** for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;

- the **network configuration and attacker emulation block**, equipped with an AI/ML-based engine, for modelling and emulation of network services, applications and security mechanisms;

- the **administration platform**, for the cyber range administrators to configure the training scenarios;

- the **digital gamified and serious game-based learning environment**, which is a simulation game framework leveraging on serious games and gamification solutions for training experts & non-expert users;

- the **risk analysis and cybersecurity economics block**, which provides the forecast for the evolution of cyber-attacks and their associated economic impact;

- the **monitoring and reporting layer**, for the **monitoring** of the **trainees' activity**, and **reporting** the **output** of the SPIDER individual components.
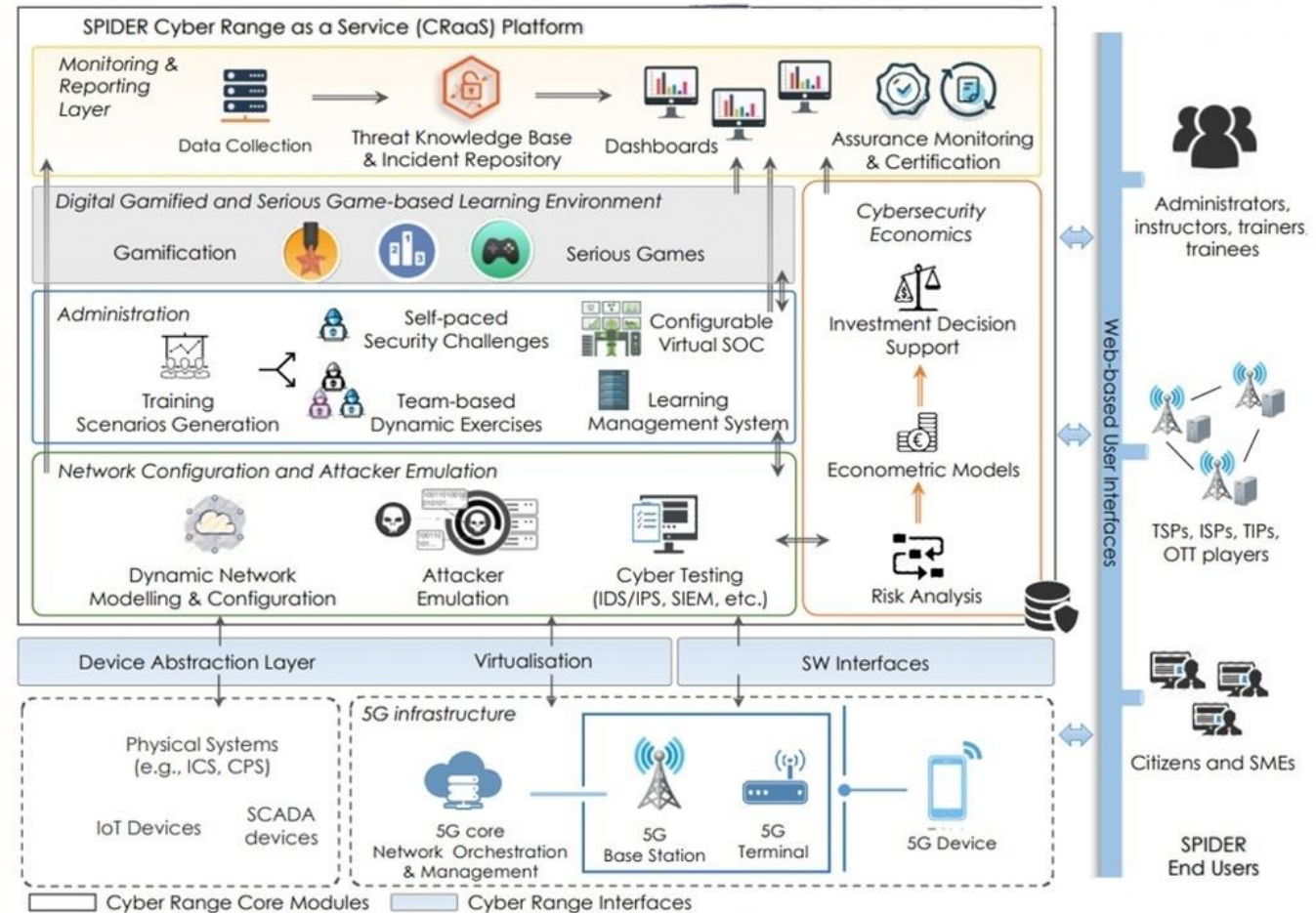
6 building blocks architecture

The proposed solution – a novel Cyber-Range Platform

- the **5G virtualisation platform** for the deployment and configuration of the network infrastructure replicating the elements for physical networking, storage, servers and test equipment;

- the **network configuration and attacker emulation block**, equipped with an AI/ML-based engine, for modelling and emulation of network services, applications and security mechanisms;

- the **administration platform**, for the cyber range administrators to configure the training scenarios;

- the **digital gamified and serious game-based learning environment**, which is a simulation game framework leveraging on serious games and gamification solutions for training experts & non-expert users;

- the **risk analysis and cybersecurity economics block**, which provides the forecast for the evolution of cyber-attacks and their associated economic impact;

- the **monitoring and reporting layer**, for the monitoring of the trainees' activity, and reporting the output of the SPIDER individual components.

6 building blocks architecture

Red/Blue Team Members

- ## Red Team
  - Ability to apply **offensive techniques** on 5G infrastructure spanning from the core to the edge of the network
  - Individual or group-based exercises
  - Monitor the progress & accelerate certification
- ## Blue Team
  - Ability to apply **defensive techniques** using traces
  - Ability to patch vulnerabilities without disrupting the running services
  - Monitor the progress & accelerate certification

Hellenic Cyber Security Team participation

- SPIDER uses of the of the **Hellenic Cyber Security** team participation for:

  - The **validation** and **extension** of the **user requirements**

  - The **evaluation** of the SPIDER **platform** as part of the pilot activities. More specifically, the Hellenic team **will join** the "**Cyber Security Experts Training**" activity

SPIDER's goal for ECSC

- SPIDER **aims** at the **exploitation** of the SPIDER platform, either during the **ECSC competition** as **part of the challenges**, or for the **purposes of training** of the **national teams**

Thank you!

Email: xenakis@unipi.gr

https://spider-h2020.eu

SPIDER.H2020/

@spiderh2020_eu