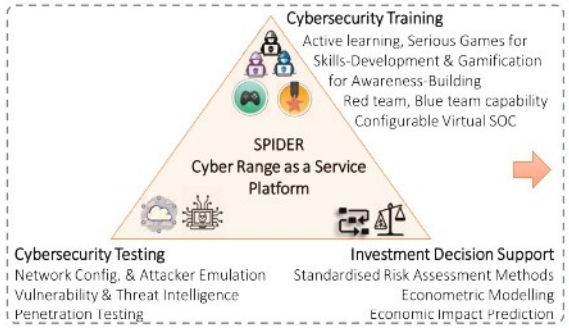
Short Description of the Project

SPIDER consortium consists from 19 [industry and academia] partners coming from 9 EU countries: Italy, Greece, Spain, France, Cyprus, UK, Denmark, Switzerland, Bulgaria. ERICSSON acts as the project coordinator.

SPIDER provides a cybersecurity platform for virtualised 5G cyber-range services, offering an innovative and holistic training experience that incorporates the specificities of 5G environments.

SPIDER's concept can be summed up on three major pillars:
[1] 5G Cyber Range Infrastructure and Supporting Technology (with a main focus on testing and assessment)
[2] 5G cybersecurity training in defending against advanced cyber-attacks both for cybersecurity experts and non-cybersecurity experts
[3] 5G Risk Analysis and Cyber security Investment Decision Support, including econometric models.



Project Duration

Start Date:
1st July 2019 – 30th June 2022 (36 months)

Project Partners

ERICSSON
cnit THALES
UBITECH ubiquitous solutions · Sphynx Technology Solutions · SERIOUS GAMES INTERACTIVE
UNIVERSITY OF PIRAEUS RESEARCH CENTER · CITY UNIVERSITY LONDON · Atos
EIGHTBELLS Independent Research & Consultancy · KEY · POLITÉCNICA
FORTH Foundation for Research & Technology - Hellas · EXALENS · Telefónica
infalia · InfoCom · uni.systems

For more information about SPIDER visit:
https://spider-h2020.eu
or scan the below barcode

Horizon 2020
European Union Funding
for Research & Innovation

SPIDER
5G CYBER RANGE

SPIDER project

Informative Brochure

Official Site
https://spider-h2020.eu

Follow us on:
https://twitter.com/spiderh2020_eu
https://www.facebook.com/SPIDER.H2020
spider-h2020-funded-project

Vision

The vision of **SPIDER** is to deliver a next-generation, extensive, and replicable cyber range platform for the telecommunications domain and its fifth generation (5G).
The envisioned platform will be offering cybersecurity emulation, training and investment decision support. Towards this vision, it features integrated tools for cyber testing including advanced emulation tools, novel training methods based on active learning as well as econometric models based on real-time emulation of modern cyber-attacks. **SPIDER** supports both self-paced and team-based exercising. Moreover, **SPIDER** acts as a serious gaming repository for multiple stakeholders to share training material and maximize efficiency in delivering complex cyber exercises. The proposed cyber range model will be validated in five highly realistic pilot use case scenarios.

SPIDER Approach

SPIDER envisages addressing the needs of two types of trainees: experts and non-experts. **SPIDER's** proposal includes serious games for 5G cybersecurity professional skills training, and gamification for 5G cybersecurity awareness training. **SPIDER** will offer a synthetic war-gaming environment engaging the trainees into playing the role of both the attacker and defender. To demonstrate the applicability and validity of the **SPIDER** platform for all requirements set by the respective funding programme (in terms of simulation, training, and economics), **SPIDER** has identified one Pilot Use Case (PUC) for each requirement (so in total 3 uses cases) including variations of them.

SPIDER Actors

While the importance of 5G and its expected adoption means that cyber-security preparedness beneficiaries will be the whole of society, each entity's perceived requirements are different.
For the individual telecommunications user, 5G is an extremely attractive proposition thanks to the high speed and ability to be connected all the time and from anywhere, where cyber-security education is an added bonus.
For a business, it is expected to increase its reliance on mobile communications (thanks to the advent of 5G) and a considerable benefit would be a reduction in cybersecurity spending and being in place to take more informed investment decisions.
For the network operators and their 5G infrastructure providers, defending against sophisticated cyber-attacks is a major concern, as a security breach. **SPIDER** will provide them an environment for testing their cyber-security defense technologies and train their employees in cyber-attacks in order to be prepared in proactively defend their assets.
For all these actors, SPIDER's Cyber Range as a Service offering can be a catalyst in ensuring cyber-security preparedness at all levels.

END USER BENEFITS

- ✔ Increased Cybersecurity Preparedness among the telecom., cloud computing, and software engineering providers
- ✔ Reduced Total Costs of Ownership through the real-time virtualisation of the network infrastructure and hosts
- ✔ Advanced Cybersecurity Protection through application of ground-breaking and market-ready security solutions
- ✔ Improved Cybersecurity Investments based on real-time risk analysis and econometric modelling

Technological Concepts

SPIDER's key technological concepts and unique selling points are:

- ✔ Development and deployment of a cutting-edge cyber range platform for instructing cybersecurity professionals in resisting and dealing with modern cybersecurity incidents
- ✔ Establishment of a realistic cybersecurity training infrastructure
- ✔ The provision of a virtual cyber environment appropriate for training on complex cyber-attacks
- ✔ The design and delivery of structured training and cyber exercises to train cyber defenders at both public and private organisations
- ✔ The delivery of a serious gaming repository for sharing training material
- ✔ The development of shared approaches to express and transform the end user needs into actual experiments and cyber exercises as well as the development of appropriate tools and methods for supporting current and future generated evidence-based simulation scenarios
- ✔ The development of unique analytics methodologies for quantifying the economic impact of cyber risk
- ✔ The derivation of improved risks analysis and econometric models to facilitate the effective decision-making and faster response to complex cyber risks
- ✔ The development of optimal risk mitigation and risk treatment methods for helping decision makers prioritise cybersecurity investments