SPIDER
5G CYBER RANGE

BRIEF SUMMARY

SPIDER NEWSLETTER ISSUE #2

We are pleased to announce the publication of the second issue of our Project newsletter!

SPIDER is a 3-year Innovation Action (IA) from 2019 to 2022 funded under Horizon 2020 focusing on delivering an innovative Cyber Range as a Service platform that extends and combines the capabilities of existing telecommunication testbeds and cyber range into a unified facility for:

- testing new security technologies
- training modern cyber defenders near-real world conditions
- supporting organisations and relevant stakeholders in making optimal cybersecurity investment decisions

The SPIDER consortium is consisted of 19 partners (industries, SMEs, research institutes and universities) coming from nine European countries: Greece, Italy, Spain, France, Cyprus, UK, Denmark, Switzerland, Bulgaria. ERICSSON acts as the project coordinator.

Despite constraints imposed from COVID-19, we can say that Year 2020 was quite positive for our project.

The SPIDER project consortium has progressed in terms of technical work and according to plan producing a number of important deliverables. Furthermore, several consortium members have attended a variety of events which attracted considerable numbers of participants. In this 2nd issue of our Newsletter, we present some of the highlights, which the consortium achieved during the last 9 months.

In the Dissemination Activities section, we present a number of online events, which we either organized ourselves or in which we participated. Also, we present a number of papers related to SPIDER, as well as some collaboration activities with other EU funded projects

TABLE OF CONTENTS

PROJECT INFORMATION

SPIDER: a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
TYPE OF ACTION: Innovation Action (IA)
GRANT AGREEMENT ID: 833685
COORDINATOR: ERICSSON, Mr. Pierluigi Polvanesi, pierluigi.polvanesi@ericsson.com
START DATE: 1st July 2019
END DATE: 30th June 2022

Stay Tuned!

on all our latest news, developments, research & general information regarding the SPIDER project.

Follow us on:

www.spider-h2020.eu spiderh2020_eu

SPIDER.H2020 SPIDER H2020 FUNDED PROJECT

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).

SPIDER
5G CYBER RANGE

PROJECT ACHIEVEMENTS

This issue covers a period of 9 months from March 2020 – December 2020 (M9 -M18). During this period of time significant progress has done in several work packages of the project.

Main achievements during this period of time were:

- Definition of reference architecture and architectural components
- Definition of the final use case scenarios
- Definition of 5G cybersecurity threat landscape and the related actors
- Functional requirements extraction and mapping to non-functional requirements
- Convert the main requirements extracted from the use cases and the specifications derived from the architecture into a set of working components
- Adapt the orchestration layer to the specificities of a cyber-range, mainly involving the automation of day-2 operations
- Creation of the required interfaces for connecting the orchestrator to external components
- Assembled a set of security assets to be appropriate for emulation scenarios, and packaged and delivered these assets as configurable artefacts in the SPIDER catalogue
- Setup of tracing and monitoring environments
- Conceptualization of serious game
- Development of a gamified training application targeted towards non-experts.
- Production of a set of four graphical cyber risk models addressing four different attacks
- Production of a report on the Cybersecurity Investment Component (CIC) of the SPIDER platform
- Elaboration on the integration perspective of the SPIDER framework
- First integrated SPIDER platform prototype has been created

Below we provide a summary per workpackage:

- **WP2 Requirements Analysis, Architecture Definition and Pilot Use Cases**

The Work Package 2 has produced a number of outputs during this period. More specifically within the WP2 context, the consortium partners conducted studies towards the analysis, collection, and extraction of the SPIDER user requirements that the architecture development must address. A fundamental step during this preliminary work was to define the 5G cybersecurity threat landscape, and the related SPIDER actors, to outline the possible attack scenarios which the SPIDER's training platform should address. Based on these outputs, functional requirements have been extracted and grouped by the identified SPIDER actors, assigned a priority. Finally, functional requirements were mapped to non-functional requirements. The use case analysis led to the definition of the respective use case scenarios.

- **WP3 Cyber Range Infrastructure and Supporting Technologies**

The Work Package 3 has reached an internal milestone, converting the main requirements extracted from the use cases and the specifications derived from the architecture into a set of working components delivered as the first technical blocks to be assembled into the early prototype of the SPIDER cyber range platform. Specifically, the work done has adapted the orchestration layer to the specificities of a cyber-range, mainly involving the automation of day-2 operations, the setup of tracing and monitoring environments, and the creation of the required interfaces for connecting the orchestrator to external components. The work performed has also seen a first breakthrough in the emulation of red team attacks via a Generative Adversarial Network (GAN) approach. A set of security assets to be employed in the definition of emulation scenarios have been assembled, packaged and delivered as configurable artefacts in the SPIDER catalogue. Finally, the data collection pipeline and the set of visualization tools to be employed in the dashboards have been defined and mocked up.

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

- **WP4 5G Cyber Security Training**

The Work Package 4 is progressing according to plan. Serious Games Interactive (SGI) based in Copenhagen acting as the Work Package 4 leader as well as tasks leader for the main training applications developed in the range of the SPIDER project spent the past months extensively researching in the field of cybersecurity training. The serious game, which is targeted mainly for the junior experts and trainees has now been conceptualised. The game play will simulate a given network that can be played as a Blue- or Red-team member in a single player session. Gaining knowledge of general defense and attack patterns are the main learning objectives. Next step is the creation of the game design document. Additionally, SGI stands as well for the development of a gamified training application targeted towards non-experts. The status is advanced and the design and wireframes have been created. The development of the application code follows.

- **WP5 Economics of 5G Security**

The Work Package 5 has already reported on a set of four graphical cyber risk models addressing four different attacks: Man-In-The-Middle, Amplification, Password brute forcing, and Privilege Escalation. These cyber risk models will be translated into machine-readable language giving as a result the corresponding four algorithms to calculate the cyber risk exposure linked to these attacks in a certain ICT infrastructure. Furthermore, WP5 has presented the Cybersecurity Investment Component (CIC) of the SPIDER platform providing at the same time detailed information regarding its functionality, cybersecurity investment decision support process as well as its interaction with other SPIDER components. Current work builds upon the Continuous Risk Analysis models and attempts to: i. complement the existing risk assessment framework via the implementation of key uncertainties underlying cyber-attacks and ii. develop optimisation and capital budgeting tools for investment in mitigation measures.

- **WP6 SPIDER Cyber Range Integration and Testing**

The Work Package 6 is progressing well and as planned. WP6 work during this period focused on elaborating on the integration perspective of the SPIDER framework and at the same time to consolidate the technical interfaces between the various components (WP2,WP3,WP4) and systems in order to ease the integration task in the SPIDER platform. The status is advanced and the First integrated SPIDER platform prototype has been created.

This consist a great challenge provided the technical review that is expected at the end of M20. Working to achieve this milestone, we have concluded technical issues such the transition of Gitlab for CI/DI pipelines from virtual to base metal environment and the access of partners to the 3 repos and we will proceed to conclude the development of simulation and emulation scenarios for specific use cases (UCs).

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

SPIDER
5G CYBER RANGE

CLUSTERING ACTIVITIES

SPIDER has initiated a collaboration with THREAT-ARREST which is also developing a general-purpose Cyber Range. The collaboration has started in July 2020 with the aim to provide a common output, concerning Cyber Ranges and Models. The output of this collaborative activity will be provided as input to the cyber range activities of the EU Cybersecurity pilot project CONCORDIA.

An early presentation of SPIDER project has been provided to CONCORDIA project in September 2020 including technical discussion on the "A modelling of the training activities for Cyber Ranges".

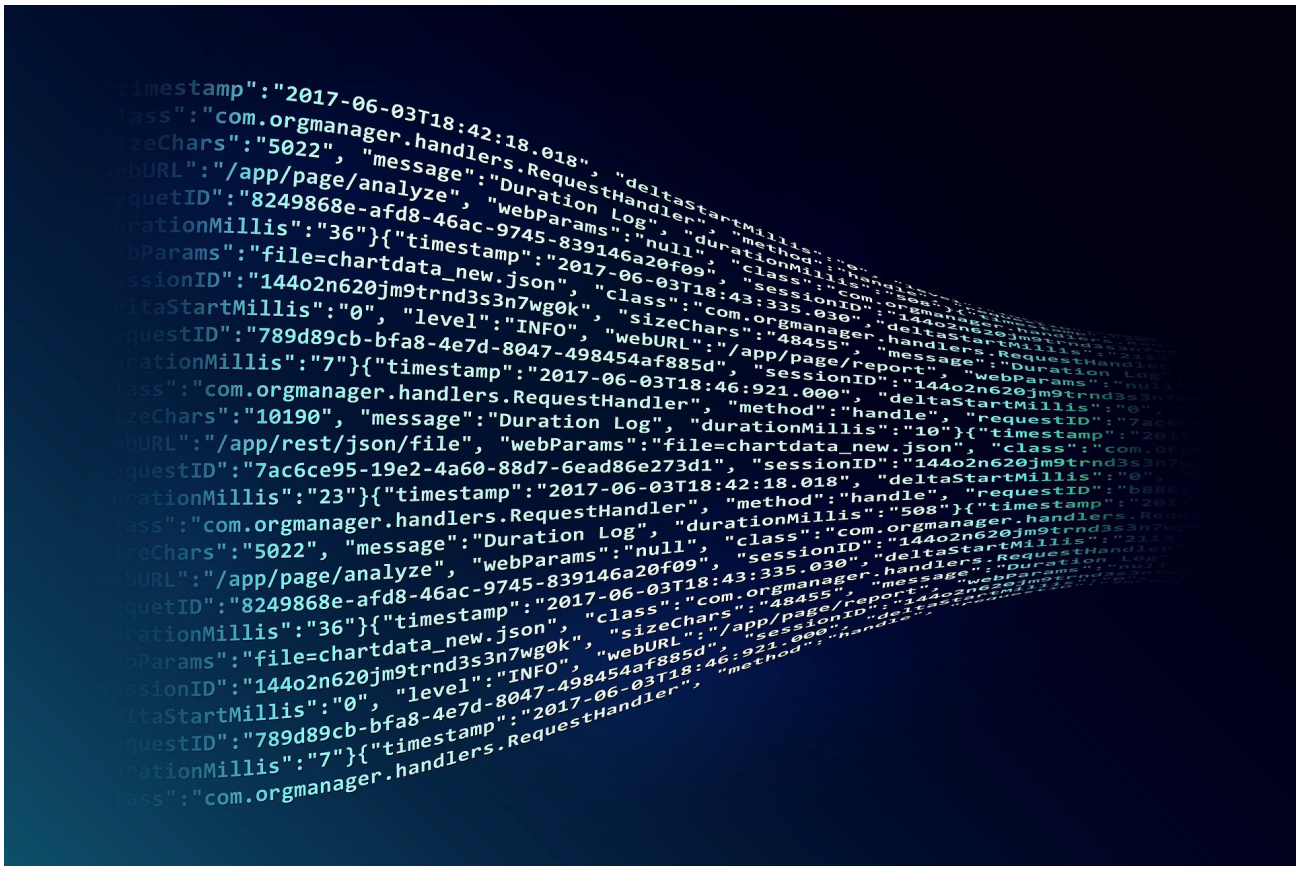
Furthermore, SPIDER has joined the CONCORDIA's Observer Stakeholder Group (OSG) with the aim to closely cooperate and interact with the CONCORDIA Consortium as well as to participate in activities and meetings of this stakeholder group.

Moreover, we have already established the "Cyber-Range Network" which is a collaborative initiative/platform created jointly from three EU funded projects: FORESIGHT, Cyber-MAR and SPIDER with the aim of (i) promoting collaboration and to facilitate exchange of knowledge among them; (ii) showcasing their respective project results to a wider audience; (iii) performing joint dissemination activities; (iv) improving overall awareness regarding cybersecurity preparedness and cybersecurity training.

In order to kick start these joint activities a joint webinar was held on November 26th where the three projects were introduced along with their key objectives and the current progress. Additionally, the concept of cyber-ranges as virtual training environments and how they can be used for cyber warfare was presented.

Finally, in the wider context of the organisation of this webinar, through the communications of the three projects, future collaboration activities' plans were discussed and agreed upon.

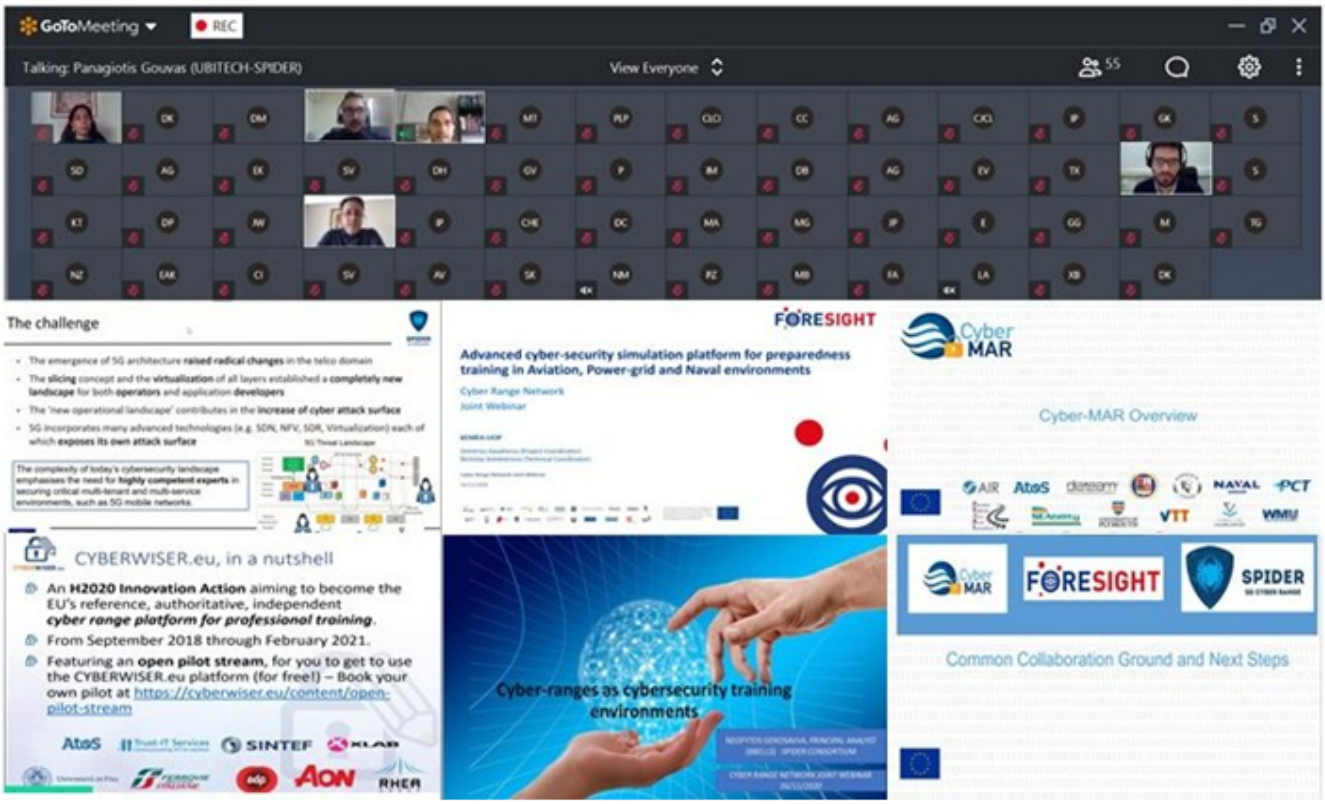
For more information about the CYBER RANGE NETWORK please visit
https://spider-h2020.eu/cyber-range-network/



The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

CYBER-RANGE NETWORK WEBINAR

CYBER-RANGE NETWORK webinar took place on November 26, having a total duration of around 2 hours. The webinar was hosted by the three projects FORESIGHT CYBER-MAR and SPIDER and was attended from around 80 participants of various backgrounds. Interesting presentations were shared by the three projects representatives describing in a comprehensive their projects current activities. The collaboration will continue through organization of future events and other activities. The event presentations will be uploaded in our website soon



14TH INTERNATIONAL CONFERENCE ON RESEARCH CHALLENGES IN INFORMATION SCIENCE (23-25 SEPTEMBER 2020)

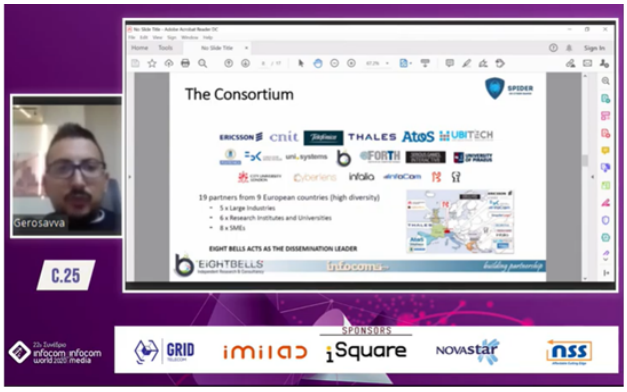
SPIDER was among the projects presented (in the form of poster) at the (virtual) 14th International Conference on Research Challenges in Information Science (RCIS 2020), an event that took place from 23-25 of September covering a variety of scientific issues. RCIS is an event organized from the University of Cyprus that brings together scientists, researchers, engineers and practitioners from a wide range of information science fields and provides opportunities for knowledge sharing and dissemination.

You can find more about the event here:
http://www.rcis-conf.com/rcis2020

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

SPIDER PRESENTATION AT THE 22ND INFOCOM WORLD CONFERENCE 2020

EIGHT BELLS delivered a virtual presentation on the SPIDER project at the 22ND INFOCOM world conference 2020 https://www.infocomworld.gr/ that took place from 4 to 6 November 2020. The conference is an annual event that is attended from the telecom, IT and media players. This year, the event took place virtually and it was focused on the upcoming 5G networks, Digital Transformation, and new technologies that will reshape the landscape.



PARTICIPATION AT THE CONCORDIA OPEN DOOR (COD) 2020

SPIDER participated as an exhibitor at the CONCORDIA Open Door 2020 (COD2020) virtual event that took place at the 28 and 29 October. COD2020 is the annual event organized by CONCORDIA and is a chance for stakeholders of all backgrounds (such as IT, entrepreneurship, education, economy, and policy) to discuss societal and technological needs in the cybersecurity field and to discover others' competences for potential collaborations.

For more information about this event please visit:
https://opendoor.concordia-h2020.eu/2020/

"5G EXPERIMENTATION FACILITIES AND VERTICAL TRIALS" WEBINAR

SPIDER was presented by our colleague from University of Piraeus (UPRC) professor Dr. Christos Xenakis at the "5G Experimentation Facilities and Vertical Trials" webinar that took place on 14/10/2020.
This online workshop was organised by the Institute of Informatics & Telecommunications of NCSR Demokritos in the frame of EU projects 5GENESIS and 5G!Drones with the support of the 5G-PPP partnership. The workshop focused on 5G Experimentation Facilities and Vertical Trials, their current status and future perspectives. The event was attended by almost 100 participants.

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

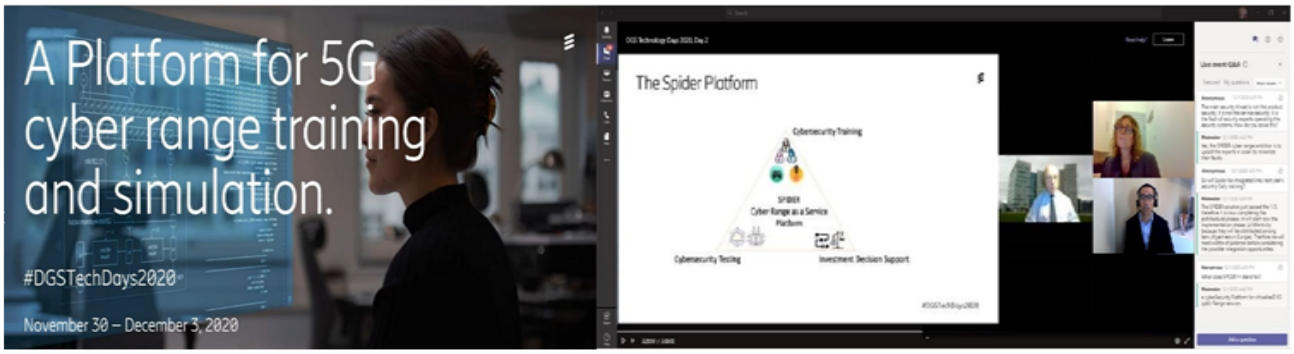
IEEE CONFERENCE ON NETWORK FUNCTION VIRTUALIZATION AND SOFTWARE DEFINED NETWORKS

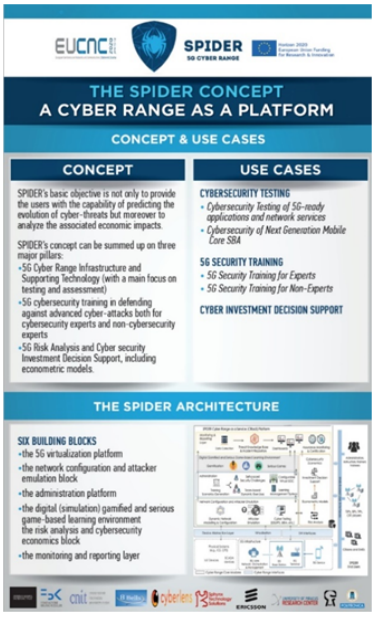
Our colleague from TID Dr. Diego R. López, delivered a keynote talk with title "Serious science and serious engineering – The way of software-based network experimentation" on the 2020 IEEE NFV-SDN conference that took virtually from 9-12 November.
IEEE Conference on Network Function Virtualization and Software Defined Networks is an important forum for the ongoing exchange of the latest ideas, developments and results amongst ecosystem partners in both academia and industry. The conference fosters knowledge sharing and discussion on new approaches as well as work addressing gaps and improvements in NFV and SDN enabled architectures, algorithms and operational frameworks for virtualized network functions and infrastructures.
For more information please visit: https://nfvsdn2020.ieee-nfvsdn.org/program/keynotes-speakers/

IEEE NFV-SDN

SPIDER AT ERICSSON DGS TECHNOLOGY DAYS 2020

Ericsson partner presented SPIDER project in a dedicated technical talk on the 1 December 2020, during the Ericsson DGS Technology Days 2020 event, that took place over four inspiring days and featured a virtual showcase of company greatest technologies, products, solutions and breakthrough innovations. The presentation was focused on the SPIDER project concept, approach and objectives. Appreciations expressed for SPIDER that has been considered a comprehensive platform
addressing security from different perspectives.





PARTICIPATION AT THE EUROPEAN CONFERENCE ON NETWORKS AND COMMUNICATIONS (EUCNC 2020)

SPIDER was presented at the Posters Sessions #2 of the EUCNC2020 event that took place virtually on 16/6 and 17/6/2020. A Video presentation and a poster (in electronic form) were prepared for attending this event.

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

Conference papers

The consortium partners CNIT, INFOCOM and FBK had papers accepted for this year's EuCNC2020 and NetSoft 2020, ICC2020 conferences, that carry acknowledgment on the SPIDER project

These papers are the following ones:

- EuCNC 2020: Operational & Experimental Insights session

Accepted paper:

- *R. Bruschi, F. Davoli, F. Díáz Bravo, C. Lombardo, S. Mangialardi and J.F. Pajo, "Validation of IaaS-based Technologies for 5G-Ready Applications Deployment"*

This paper was presented on 16/6/2020 at the EUCNC2020 sessions of Operational and experimental insights.

EUCNC 2020 June 15-18
European Conference on Networks and Communications | Dubrovnik, Croatia

- NetSoft 2020: Short Papers Track https://netsoft2020.ieee-netsoft.org/

Accepted papers:

- *R. Bolla, R. Bruschi, F. Davoli, C. Lombardo and J.F. Pajo, "Debunking the "Green" NFV Myth: An Assessment of the Virtualization Sustainability in Radio Access Networks" (paper from CNIT partners)*
- *R. Bruschi, F. Davoli, G. Lamanna, C. Lombardo, S. Mangialardi and J.F. Pajo, "Enabling Edge Computing Deployment in 4G and Beyond" (paper from CNIT + INFOCOM partners)*

IEEE NETSOFT
IEEE Conference on Network Softwarization
29 June-3 July 2020 // Virtual Conference
Bridging the Gap between AI and Network Softwarization

- 5th IEEE ICC 2020 Workshop on Convergent Internet of Things https://icc2020.ieee-icc.org/

Accepted paper:

- *Cristina E. Costa, Marco Centenaro and Roberto Riggio, "LoMM: a Monitoring and Management Platform for LoRaWAN Experimentation," 2020 IEEE International Conference on Communications Workshops (4th Workshop on Convergent Internet of Things (C-IoT)), Dublin, Ireland, June 2020 (paper from FBK partners)*

The event took place from 7-11/6/2020 and the paper presentation was available as video on demand until the end of the month.

IEEE ICC
IEEE International Conference on Communications
7-11 June 2020 // Virtual Conference
Communications Enabling Shared Understanding

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

Journal papers

• IEEE ACCESS/ "Detection of encrypted cryptomining malware connections with machine and deep learning".

Our partners TID and UPM got a paper accepted and published in open-access mode for the IEEE-Access journal with title: "Detection of encrypted cryptomining malware connections with machine and deep learning". This paper carries acknowledgement of the SPIDER project. This paper is available in open access mode below: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9178288

• IEEE ACCESS / "On identifying threats and quantifying cybersecurity risks of MNOs deploying heterogeneous RATs"

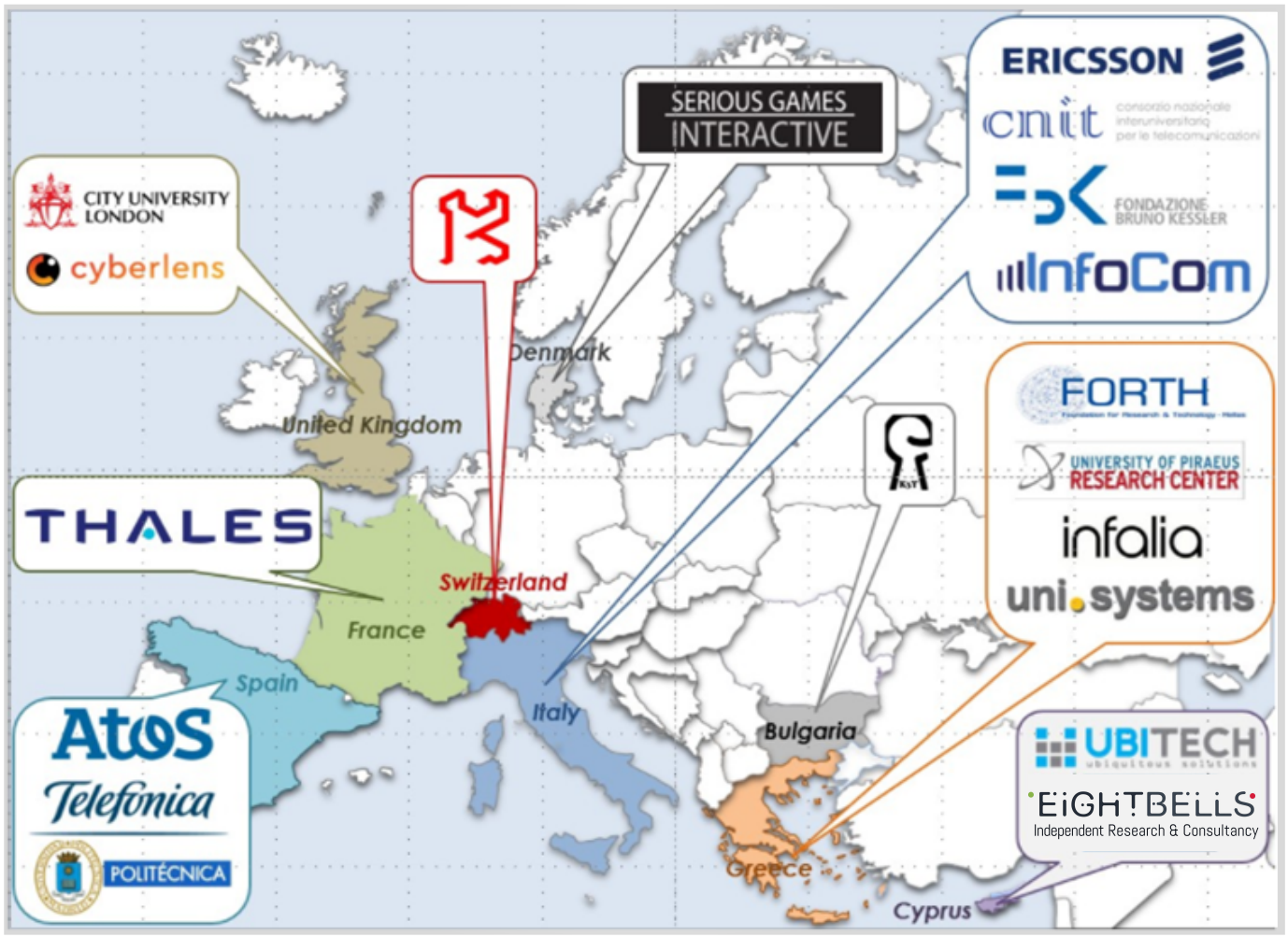
Our partners from University of Piraeus (UPRC) got a paper accepted and published in open-access mode for the IEEE-Access journal with title "On identifying threats and quantifying cybersecurity risks of MNOs deploying heterogeneous RATs". This paper acknowledges SPIDER and is available in open access mode under the link:
https://ieeexplore.ieee.org/document/9296264

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains

SPIDER
5G CYBER RANGE

WEBSITE & SOCIAL MEDIA



Please find more information about SPIDER:

www.spider-h2020.eu

spiderh2020_eu

SPIDER.H2020

SPIDER H2020 FUNDED PROJECT

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n°833685 (SPIDER).
The document reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains