a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

Deliverable D1.5

Report on awareness and wider societal implications

Grant Agreement number:	833685
Project acronym:	SPIDER
Project title:	a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services
Start date of the project:	01/07/2019
Duration of the project:	36 months
Type of Action:	Innovation Action (IA)
Project Coordinator:	Name: Pier Luigi Polvanesi Phone: +39 010 600 2662 e-mail: pierluigi.polvanesi@ericsson.com

Due Date of Delivery:	31/12/2021
Actual Date of Delivery:	22/12/2021
Work Package:	WP1
Type of the Deliverable:	Report
Dissemination level:	Public (PU)
Main Editors:	ERICSSON
Version:	1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833685.

List of Authors, Contributors, Reviewers

Name	Role	Organization
Leading Authors	Pier Luigi Polvanesi	ERICSSON
Co-Authors	Massimo Enrico	ERICSSON
Contributor	Eirini Karapistoli	CYBERLENS
Reviewer	Ioannis Tsampoulatidis	INFALIA
Reviewer	Konstantina Papachristopoulou	8BELLS

History of changes

Version	Date	Change History	Authors	Organization
0.1	01/09/2021	Initial Version, drafting TOC	Pier Luigi Polvanesi	ERICSSON
0.2	18/10/2021	Early draft of deliverable content	Pier Luigi Polvanesi	ERICSSON
0.3	29/10/2021	Second draft	Pier Luigi Polvanesi	ERICSSON
0.4	22/11/2021	Third draft - thorough revision	Pier Luigi Polvanesi	ERICSSON
0.5	29/11/2021	Content available for all the foreseen ToC sections	Pier Luigi Polvanesi	ERICSSON
0.6	06/12/2021	Fixed comments received	Pier Luigi Polvanesi	ERICSSON
1.0	22/12/2021	Final version for submission	Pier Luigi Polvanesi	ERICSSON

Disclaimer

The information, documentation and figures available in this deliverable are written by the SPIDER Consortium partners under EC co-financing (Call: H2020-SU-DS-2018, Project ID: 833685) and do not necessarily reflect the view of the European Commission.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability.

Table of Contents

1 Executive Summary 9
2 Introduction 10
2.1 SPIDER overview 10
2.2 Structure of the Deliverable 11
3 SPIDER Value Proposition 12
3.1 Innovations 13
4 SPIDER Awareness Framework 17
4.1 Dissemination and Communication Activities 18
4.1.1 Social Media and Website 19
4.1.2 Dissemination Material Representing the Project 22
4.1.3 Activities and Events 23
4.1.4 Papers, Journal Articles and Posters 24
4.1.5 Papers -Open Access 26
4.1.6 SPIDER Whitepaper 26
4.1.7 Other Activities 27
4.2 Market analysis and exploitation 31
4.3 Standardization 32
4.4 Liaison with Stakeholders and Creation of Operational Links with EU CERTs/CSIRTs 33
4.5 Deliverables of the awareness framework 33
5 SPIDER Practical and Social Implications 35
5.1 Practical Implications 35
5.1.1 Feature value proposition based on learning modalities 36
5.1.2 Architecture walkthrough & SPIDER Actors 36
5.2 Pilot Use cases 37
5.2.1 PUC1: Cybersecurity Testing 37
5.2.2 PUC2: 5G Security Training 38
5.2.3 PUC3: Cybersecurity Investment Decision Support 39
5.3 Evaluation methodology and measures specifications 40
5.3.1 Metrics and KPIs Framework 40
5.3.2 Perceived Quality of Experience Metrics Framework 41
5.4 Social Implications 42
6 Gender Issues 44
7 Conclusions 45
References 46

List of Tables

Table 1 - Dissemination activities' status........18
Table 2 – Events participated by consortium members during the first year of the project........23
Table 3 – Events participated by consortium members during the 2nd year of the project........24
Table 4 – Events participated by consortium members during M25-M29 of the project........24
Table 5 - List of SPIDER scientific peer reviewed publications........25
Table 6 - SPIDER Actors........37

List of Figures

Figure 1: SPIDER Dissemination activities GANTT CHART defined in D8.1........18
Figure 2: Website homepage........20
Figure 3: SPIDER Facebook page........21
Figure 4: SPIDER Twitter page........21
Figure 5: SPIDER Linkedin account........22
Figure 6: SPIDER publications available in open access on the Zenodo website........26
Figure 7: The CYBER RANGE Network........27
Figure 8: The registration form of the joint webinar........27
Figure 9: The CRST workshop logo and supporting projects........28
Figure 10: CERTs/ CSIRTs that have attended the 2 workshops........29
Figure 11: CONCORDIA logo........29

Glossary

Acronym	Explanation
3GPP	3rd Generation Partnership Project
5G-PPP	5G Infrastructure Public Private Partnership
AI	Artificial Intelligence
CERTs	Computer emergency response teams
CAPEC	Common Attack Pattern Enumeration and Classification
CRAE	Continuous Risk Analysis Engine
CIC	Cyber Security Investment Component
CRaaS	Cyber Range as a Service
CSIRT	Computer security incident response teams
DoW	Description of Work
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DL	Deep Learning
DSP	Digital service providers
ENI	Experiential Networked Intelligence
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
EU	European Union
EUCNC	European Conference on Networks and Communications.
ETSI	European Telecommunications Standards Institute
GAN	Generative Adversarial Networks
GDPR	General Data Protection Regulation
IA	Innovation Action
ICT	Information and Communications Technology
IEEE CSR	IEEE International Conference on Cyber Security and Resilience
IEEE ICC	IEEE International Conference on Communications
IETF	Internet Engineering Task Force
IJIS	International Journal of Information Security
ISP	Internet Service Providers
JCR	Journal Citation Reports
KPI	Key Performance Indicators
ML	Machine Learning
MNO	Mobile Network Operator
NETSOFT	IEEE Conference on Network Softwarization
NF	Network Function

NFV	Network function Virtualization
NFVO	Network function Virtualization Orchestrator
NIS	Network and Information Security
OES	Operators of essential services
OTT	Over-The-Top player
OSM	Open-Source MANO
OSS	Operation Support Systems
PNF	Physical network functions
RCIS	Research Challenges in Information Science Conference
QoE	Quality of Experience
QoS	Quality of Service
SAP	Security Assurance Platform
SBA	Service Based Architecture
SBI	Service Based Interface
SDN	Software Defined Networking
SIEM	Security information and event management
SOC	Security Operations Centre
SSLA	Security Service Level Agreements
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TEE	Trusted Execution Environments
TIP	Telecom Infrastructure Providers
TSP	Telecom Service Providers
USD	United States dollars
USRP	Universal Software Radio Peripheral
VNF	Virtual network functions
VAO	Vertical Application Orchestrator
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
vSOC	virtualized Security Operation Center
WIM	Wide-area Infrastructure Manager
WP	Work Package
ZSM	Zero-touch network and Service Management

1 Executive Summary

This deliverable represents the report on **awareness and wider societal implications of the SPIDER project at M30**. The aim of the report is to assess the results of the work conducted within SPIDER in relation to **practical as well as socially impacting issues** and to provide specific information on **how gender issues were carefully addressed by the project**.

The **vision of SPIDER** is to deliver a next-generation, extensive, and replicable cyber range platform tailored for the telecommunications domain, offering multi-modal training. 5G infrastructure relies on the latest developments of virtualization technologies. In practical terms, the heart of such networks relies on the transformation towards adoption of software-based solutions on all 'traditional' layers, from the backhaul to the very front-end (i.e., radio part). However, as an immediate consequence is that such a paradigm shift contributed to a radical increase of the exposed cyber-security attack vectors. In fact, the entire ecosystem, while it is undoubtedly much more versatile and flexible, as far its management is concerned, can be a potential target to adversaries.

Under this perspective, **training has become extremely important**. When it comes to the concept of training, it should be clarified that SPIDER objective is to extend its most immediate target group of ethical hackers/experts, that aim to leverage their competences, including an increased audience covering risk assessors and non-expert users. To this end, SPIDER aims to cover holistically the cyber security niche requirements of the 5G domain.

The **educational value proposition of SPIDER is articulated over 4 distinct learning modalities**, namely: Modality-1 (Theoretical training), Modality-2 (Emulation-based training), Modality-3 (Simulation-based training) and Modality-4 (Security-awareness training).

On the one hand, the present report summarises **the values and benefits coming from the SPIDER solution**, which has been realized within the course of the project, and have clear and positive impact on various areas on the envisaged target markets.

On the other hand, it provides **a summary overview of the various activities that took place during the lifecycle of SPIDER project** until the time of writing this report, i.e. M30 (Dec '21), to realize an **explicit awareness of the pursued research and associated solutions within an extended variety of sectors, events and communication channels**.

Finally, this deliverable analyses the **implications from a practical point of view** providing both a technical perspective of the SPIDER platform centred on its learning modalities offering, and a description of the demonstration strategy based on validation use cases and related methodology. Concerning the **societal implications** an analysis is provided on how SPIDER solution aims to assist the next generation of telecommunication organisations ensuring a more cyber secure environment for all EU citizens. Also, this deliverable is concluding with a **prospect on the gender issue** and standpoint within the consortium.

2 INTRODUCTION

2.1 SPIDER OVERVIEW

Modern societies have become increasingly dependent upon critical (cyber) infrastructures, and this dependency is only becoming stronger as ICT progress. As the future of the telecommunications sector, 5G network infrastructures are key critical information infrastructures, with Telecom Service Providers (TSPs), Internet Service Providers (ISPs), cloud infrastructure providers, and Over-The-Top (OTT) players, depending upon such infrastructures, and comprising one of the backbones of Europe's economic growth.

SPIDER has developed a cyber-arena where ethical hackers can leverage their skills on top of modern 5G networks using realistic hacking scenarios. 5G networks rely heavily on virtualization technology and as such modern networks expose increased attack vectors. These attack vectors can be exploited by hackers to manipulate modern infrastructure. The specificities of the 5G environment (usage of software defined radio, programmable slices) prevent the ability of a holistic training experience for a trainee. SPIDER covers this gap through the development of an innovative platform which offers:

- the ability to conduct exercises in a realistic environment that emulates real 5G deployments where all 5G-integral components are present. Such an environment can be parameterized and spawned on-demand by materializing a specific slice configuration.
- the ability to automatically infer performance tracking of trainees and the extraction of their learning gaps.
- the ability to provide self-paced learning regarding theoretical aspects of security through a serious game.

With the goal to address the impact on the preparedness of security professionals, SPIDER offers a powerful training environment for improving technical security skills through a variety of cyber exercises. SPIDER's innovative virtual cyberwarfare training environment helps the next generation of cyber defenders to advance their cybersecurity skills and better prepare to respond to emerging cyber-attacks by testing and evaluating (under high-stress, and real-world conditions) security technologies and methodologies.

To this end, SPIDER offers four distinct educational modalities which include:

- **Modality 1 – Theoretical Training**: It is the type of interaction according to which the trainee is served with a set of **theoretical/comprehension questions** (on a specific 5G sub-domain of security) to assess his/her theoretical skills.

- **Modality 2 - Emulation Training**: It is the type of interaction according to which the trainee(s) are asked to i**nteract physically** with a target deployed by SPIDER, with the goal of hacking it (for Red teams) or defending it (for Blue teams).

- **Modality 3 - Simulation Training through a Serious Game**: It is the type of interaction according to which trainees **calculate risks and evaluate countermeasures on top of hypothetical deployment** of interconnected vulnerable assets with the endmost goal of minimising risk subject to specific cost and resources.

- **Modality 4 - Security Awareness Training through Gamification**: It is the type of training targeting non-expert users that aim to acquire some **fundamental technical skills** that are essential in the security domain (e.g., password strengths, usage of encrypted tunnels).

Furthermore, due to the increasing cyber-risk and economic uncertainty, organizations that rely heavily on IT infrastructures require managerial strategies that are responsive to market conditions. Accordingly, improved knowledge on how organizations can make the right investment to secure their operations against cyber-attacks should be a priority for modern ICT organizations. SPIDER's mission goes well beyond permitting a multidisciplinary understanding of the costs and investment decisions around securing information systems, enabling organizations to better shape their cybersecurity budget spending strategies towards securing their operations against cyber-attacks.

Ultimately, SPIDER will contribute towards enhanced economic performance through encouraging further development and path to market for integrated cyber range solutions. The enhanced economic situation will also have a catalyzing social impact through improved incomes and enhanced societal conditions within a wider societal context. In general, effective preparedness against emerging cyber threats is a business enabler, as it creates a safe environment for business.

2.2 STRUCTURE OF THE DELIVERABLE

The document is segmented into 4 main sections.

Section 2 (this section) introduces the deliverable.

Section 3 provides an overview of the **value proposition** coming from the SPIDER solution that derives from the market analysis conducted during the project.

Section 4 focuses on the **awareness framework** adopted and developed through the various dissemination and communications activities to realize wide awareness of the project in the target sectors. This includes exploitation and standardization activities carefully organised and consequently carried-out within the project.

Section 5 is about the **implications from a practical and societal point of view**. This part elaborates on how the outcome of SPIDER is aimed to assist security professionals of various levels (expert, intermediate, and novice) to leverage their skills. It also provides a view of the practical implication of positioning SPIDER into the 5G ecosystem. Furthermore, this section outlines the positive societal impacts of the SPIDER solution that is designed to assist the next generation of telecommunication organisations to better prepare against complex cyber-attacks.

Section 6 addresses the **gender balance in research teams** dealing with female representation and support in promoting equal employment opportunities among the partners organizations.

Finally, **Section 7** concludes this deliverable.

3 SPIDER VALUE PROPOSITION

Some clear trends are underway in the cyber range market as outlined by the competitor analysis presented in Deliverable D8.3 "Interim Report on dissemination, communication, standardisation, and exploitation" [9] available since June 2021.

The model of delivery as-a-service, cyber threats and an advanced tool for the value and assessment of cyber risk, the integration of 5G assets, gamification strategies, the learning path of trainees, specialization in the 5G market are the foundational values of SPIDER. It has the ambition to extend the innovation in these fields and make a competitive entrance in the market

The SPIDER capabilities considered relevant for the solution created by the project are presented below. The functions of SPIDER are combined with their value proposition with respect to the relative market trends.

*SPIDER has supported the **as-a-service delivery model**, taking full use of the latest virtualization techniques and remote access to the range. The selected model takes full advantage to make the cyber range usable to many potential customers and use it to enter B2B markets.*

In this respect, considerations can be given to the first market trend that is represented by the transition to the cloud by offering *as-a-service* models, in which users connect remotely to the computer range via an Internet connection and a web browser. This marks a clear departure from the standalone mode that has been the rule in the past, where computer ranges were developed without deviations locally at the customer or at the supplier side. The *as-a-service* models are the best way to train start-ups and SMEs and it seems to be strategically effective in attracting new customers by lowering the usual entrance barriers for local cyber-ranges (i.e., high costs for creating the environment and/or booking training slots in places). One of the disadvantages is the reduction of the depth of operation for specific content, for example, SCADA security, Wi-Fi vulnerabilities, and vulnerabilities of radio protocols. Large enterprises are increasingly using a hybrid approach by offering both cloud-based and traditional on-premises computing ranges, often based on the same technologies.

*SPIDER includes in its architecture the **ability to share information about cyber threats and an advanced tool for cyber risk value and assessment**. These two represent cutting-edge solutions developed specifically for SPIDER.*

From a market perspective, among the common trends that appear from the analysis it can be recorded the integration of cyber threat information collection and sharing modules to present and train the latest vulnerabilities and attack techniques. Cyber risk assessment tools have also begun to appear in commercial products, such as methods to identify key assets and assess how to better protect them.

One key aspect of SPIDER capabilities is the ***integration of 5G assets (e.g. RAN, 5G cores, MEC, Orchestrators) into training scenarios*** *which is also representing one of the pillars of the planned go to market strategy.*

This SPIDER capability becomes a unique selling point as an extension of the following market trend. A key point of differentiation is the inclusion of cybersecurity resources generally used through partnership agreements between cyber range developers and providers of cybersecurity assets. This allows trainees to hone their computer skills on the same tools used in production, while also allowing them to create specific certification programs. The integration of these resources is also a key advantage for those companies that develop security resources close to computer ranges, allowing them to use the cyber range to market their products and gain users.

SPIDER offers much of the work effort to the ***development of gamification strategies related to the learning path of the trainees, both in simulation and in emulation modes****. A mix of cloud orchestration technologies and specific developments contributes to facilitate the deployment. The customization of specific 5G scenarios is documented through pilots.*

This is aligned with the approach to gamification that is evaluated by all cyber range providers as key means to make the learning experience enjoyable, collaborating to retain users, giving them new and interesting challenges. What's more, all competitors emphasize the ease of implementation and use of their platform and the ability to customize the training experience to suit any customer need through specialized content. This marketing is tied to the current key pain points of cybernetic range platforms, namely the complexity of creating and implementing a representative training scenario.

An aspect which is relevant for SPIDER is the ***clear specialization in the 5G market, which represents an important niche****. Due to the structuring nature of 5G, it is also expected that most other verticals will embrace 5G in the next coming years.*

This perspective is strongly supported by the analysis of the cyber range market where we can see that in recent years, we have seen a shift from cyber ranges oriented to generic IT training on cybersecurity, to those aimed at a specific segment of the market (vertical). This has created a multitude of niche markets, in which one or two suppliers specialize. Niche categories range from defense, finance, gas & oil, transportation, energy and utilities, industry, each proposing specific use cases and access to different assets.

3.1 INNOVATIONS

SPIDER is an Innovation Action (IA) that is making a leap forward in several knowledge areas spinning around cybersecurity and in particular the delivery of cyber training capabilities. The different innovation streams identified within SPIDER are presented below.

- **SPIDER is a cyber range focused on 5G, not a generalist one:** Cyber ranges constitute a flourishing market and most existing platforms are conceived in a generalist way, providing cross knowledge from the basics to advanced levels. Leveraging knowledge and experience acquired in recent years, the SPIDER Consortium focuses on the telecom sector, particularly on 5G communications, expected to represent key technological enablers for several vertical industries in the next decade. While there are no works on cyber ranges focused on 5G cybersecurity, SPIDER covers the whole chain of end-to-end services, from the end-device up to the application deployed in the cloud, via the radio access and the core networks. The ability to interact with a real 5G deployment is extremely valuable since it unleashes the potential of experienced users to perform sophisticated attacks that include pivoting and escalation techniques.

- **SPIDER is a cyber range that follows a hybrid approach combining both emulation and simulation techniques:** Regarding emulation, SPIDER offers high flexibility to deal with a wide range of situations with respect to resources availability. In the likeliest situations, it is not possible to count on real 5G equipment to materialize a scenario in the frame of a training exercise. This is solved thanks to virtualization and the ability to recreate different networked interconnected assets playing different roles in the emulated infrastructures. On the other hand, it offers the possibility to support scenarios where virtualized services (e.g., a virtual Evolved Packet Core - EPC) and physical assets (e.g., a Universal Software Radio Peripheral - USRP module) are both configured; since an interplay between them is required for sophisticated exercises. This is fully in line with the existing trend of creating, not only virtual-physical arenas associations, but also federations of cyber ranges that share resources and make each other more powerful to deliver highly sophisticated cyber training. The Vertical Application Orchestrator (VAO) is the component that handles the choreography of service-graph lifecycle management from initial deployment to final resources release. To support emulation exercises, a key element is the virtualized Security Operation Center (vSOC), which is explicitly designed to monitor inbound and outbound network traffic and allow pre-emptive actions for the members of the blue team. On the other hand, the serious game comprises the simulation that aims to create an environment/level/network where essentially all sorts of security scenarios could be possible to train.

- **Provision of self-paced learning through gamification:** The application of gamification to cybersecurity training is a very innovative pathway to explore in depth. The amusing component of these games eases the engagement of the trainee, the acquisition of the knowledge and its eventual retention. The game elements are closely tied to what the user already does in the real world. It is a way to focus more clearly on the right behaviour, get feedback when things done right, and get motivated by seeing clear progress in the form of level-ups, achievements or similar. Like real-life, the blue team (more like a corporation) is made available more resources to use in the game whereas the red team (more like an activist hacker group) has a smaller set of resources. This type of training is an easy opportunity to practice cybersecurity strategies and management, abstracting away the complexity of using very specific technical tools. In addition, it eases the provision of self-training. It is worthwhile to train the employees in information security. It must be possible to trust that employees understand information security and that they can understand the intentions and methods of criminals. For non-experts, SPIDER gamification solution gives the chance to offer training in small daily learning pills (microlearning), easy to digest, in which the employees adopt an active role in their learning process, increasing retention and easing the transfer of knowledge. Security threats and attacks are ongoing and typically the "weakest link" the non-experts are exploited.

- **Live library of 5G components to emulate which can be parameterized and spawned on demand:** The project has an innovation stream addressing the need to characterize with greater fidelity different 5G components. These bricks are employed to build realistic fully fledged 5G infrastructures in the most-common case when real-world components cannot be used for experimentation and training. The programmable infrastructure offered by SPIDER plays a key role to make it possible. SPIDER uses Virtual Network Functions (VNFs), Physical Network Functions (PNFs) or virtual applications for the slices. The flexibility of this library enables the support of multiple use cases.

- **Live library of 5G fully focused scenarios:** Assembling the different bricks available in the component library, and always keeping the possibility to make them interoperable with real elements, SPIDER offers a library of 5G fully focused scenarios ready to be used to run a practical training on top of them. It is important not to forget that SPIDER not only addresses training, but also testing, and can be used to test new security technologies. Finally, SPIDER also offers scenarios targeting risk managers to provide proper support to optimally decide on the best investments to strengthen corporate infrastructures against potential cyber threats and attacks. In this sense, different cyber risk models focused on highly relevant attacks to 5G infrastructures are developed during the project lifecycle. SPIDER contributes to ease the decision-making process on how to configure the corporate cybersecurity investment. SPIDER brings innovative intelligence for control selection, which is able to compute the optimal set of controls given a fixed budget. This feature can assist in the discussion between technical and managerial teams prior to those investments.

- **Usage of Artificial Intelligence / Machine Learning to train models that can be used for sophisticated offensive or defensive activities:** For attacking, Generative Adversarial Networks (GANs) is a variant that is available to generate synthetic network attacks that are different to each other yet with similar statistical characteristics. This tool can be used in emulation scenarios and the traffic generated is highly realistic. It addresses a recurrent problem for cyber ranges, which used to have to trust 3rd party components to obtain this traffic which is fundamental for emulation exercises and/or bring specialized red-teamers to inject this traffic directly in the emulation. These options increased the cost of cyber ranges and hindered its adoption in companies with less economic resources. Unlike hardware solutions, this virtual solution is affordable and customizable with the downside of the lower performance in comparison with hardware tools for the same purpose. Unlike the prevailing existing data augmentation solutions, we obtain synthetic flow-based traffic that can fully replace real data. Therefore, this solution can be applied in scenarios where data privacy must be guaranteed. For defending, Machine Learning is applied to support early detection of cybersecurity threats and the defense of the network infrastructure. User will learn how to use with new ML based tools. The SPIDER platform contains a Machine Learning Lab which is a key asset of its value proposition. This lab is used to create offensive and defensive "primitives" to be used in the emulation scenarios. It is supported by a Machine Learning Orchestrator that works offline to train specific models that can be used to work out such "primitives".

- **Possibility for trainees to bring their own tools:** The SPIDER platform offers the chance to incorporate third party tools that are not included in the set SPIDER makes available for the trainees. This way the trainee can benefit from a more customized learning experience, as well as bridge possible gaps existing in the SPIDER platform. This is applicable to both the red and blue team members.

- **Automatic scoring system embedded in the platform, and specific to each scenario:** SPIDER uses as much as possible information logged during the execution of an exercise to automate the evaluation of performance for user/s teams involved in the exercise. The performance evaluation system is very adaptable to the needs of each scenario, considering the type of information that will be available to make such an evaluation. In the case of defensive actions performed by the blue team, not only the action itself will be evaluated, but also its cost and potential benefit. In practical terms, rather than a vanilla scoring system, there will be different flavors fully aligned with the scenario in question with a high degree of customization. The system is continuously giving the users feedback about the effect of their actions, therefore they will never find themselves lost in the dark. Additionally, the platform can automatically assess the level of expertise of the user and assign upcoming exercises according to such a level, also considering the detected learning gaps the platform is able to identify (with no human in the loop). SPIDER welcomes users from a very wide range of expertise levels, from non-experts to highly experienced people who seek to improve their preparation for major cyber incidents.

- **SPIDER security self-monitored and certified**: Despite the nice catalogue of cool features and different innovation streams converging in the SPIDER cyber range platform, it would be useless if security was not at the core of the design and implementation process. SPIDER incorporates a Security Assurance Platform (SAP) as reported in D5.2 “SPIDER assurance and certification monitoring solutions” [4], which is a horizontal component responsible to monitor and assess the security of the SPIDER platform. It ensures the security and the privacy of the data held in the SPIDER platform. It provides a real-time view of the security posture of the 5G testbed. This mechanism assures the confidentiality, integrity, and availability, which are continuously monitored basing on gathered events and Event Calculus logic. It applies to data (both in-transit and at-rest) and at the level of platform components (e.g., authentication and non-repudiation of distributed platform components).

4 SPIDER AWARENESS FRAMEWORK

Since the beginning, the SPIDER project has focused on the development and execution of viable plans for the **communication, dissemination and exploitation activities** that are reviewed and updated regularly. The objective is to achieve high measurable impact of the project results and ultimately, to lead to a successful adoption of the SPIDER cyber range innovative features into the 5G evolution ecosystem. It is important to highlight that while the COVID-19 pandemic has significantly affected some of the awareness activities in the first half of the project, at the same time it has contributed to establish a different approach in conducting dissemination with the systematic adoption of virtual communication platforms as an alternative approach to the physical presence in the majority of the cases.

The awareness framework of SPIDER organizes the different aspects of the established plan of activities grouping them into tasks. The main task undertakes **project dissemination and all public communication outreach activities**, mainly focusing on the various forms of publicly representing SPIDER on the internet, on the events, conferences, webinar and workshops, and on the journal articles and scientific papers.

Other two additional tasks are oriented into addressing more specific awareness line of actions. One is dedicated to **coordinating and organizing contribution to standardisation groups**, including standardisation bodies and open-source communities and another one aims to **create liaisons with several security related stakeholders** from Industry, SMEs and the Public Sector. The most concrete outcome of the latter task has been in establishing relationships with other cyber-security related projects for common initiatives and setting up operational links between SPIDER and various EU CERTs/CSIRTs.

Finally, another task addresses an important aspect of the SPIDER exploitation plan, dealing with the **exploration of the means of delivering the SPIDER innovations to the market**. A continuous market analysis is conducted towards deriving the factors that will facilitate SPIDER's market adoption.

The work carried out so far produced a preliminary exploitation plan for the assets identified with a specific description of the proposing organization background and the general strategy of exploitation for each outcome of the project. A first elaboration of the market analysis for SPIDER covers among others the identification of the requirements of the 5G in terms of cybersecurity in comparison with past generation mobile networks, the benefits of a cyber-range dedicated to 5G, which are evaluated in connection with the value proposition of SPIDER, the competition analysis for cyber range and the market outlook in the target segments such as cyber security, cyber training and education, 5G network and applications.

4.1 Dissemination and Communication Activities

In Figure 1: SPIDER Dissemination activities GANTT CHART defined in D8.1 below a Gantt chart is presented that was originally defined at the early stages of the project as part of D8.1 "Plans for dissemination, communication, standardization and exploitation" [7] to summarize all the communication and dissemination activities and provide a tentative timeline for the implementation of the project's various dissemination activities. Depending on the project progress status and the availability of the project results some activities may be shifted at a later project stage. One clear evidence was that due to COVID 19 impact almost all activities from M8-M24 took place online.

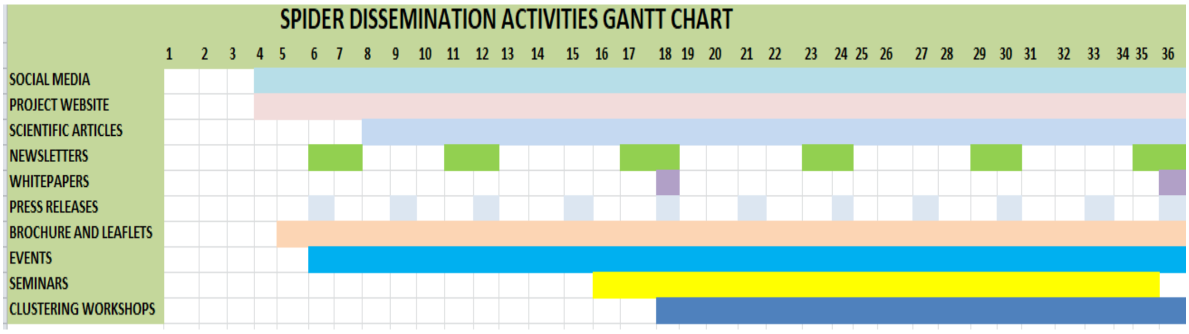


Figure 1: SPIDER Dissemination activities GANTT CHART defined in D8.1

A prospect of the activities during the first 30 months of the project lifecycle is presented in Table 1, below.

Table 1 - Dissemination activities' status

Type	Description	Status up to M30
Project awareness and Scientific Knowledge Transfer, Research Papers, Whitepapers	Participation to or organization of scientific events, conferences and workshops as well as participation to industry interest groups, venues, associations and standards' bodies events.	PARTICIPATION: 37 events of various types (workshops, conferences, trainings etc) attended -17 attended events during YEAR 1 -15 attended events during YEAR 2 - 5 attended events during early six months of YEAR 3
Scientific publications	Publication of papers in journals and magazines.	Overall, 15 accepted publications acknowledging SPIDER -9 papers for conferences accepted -6 papers for journals accepted
Whitepapers	Whitepapers available on social media platforms and the project's website.	Whitepaper #1 released
Marketing Material	Leaflets, Posters, Brochures, Press Releases, Videos	AVAILABLE: Leaflet, Brochure, - Posters available at the project website - 3 videos (including a webinar) uploaded to the YouTube channel
Project Website	Raising awareness of SPIDER	Website available early on and constantly updated

Social Media	Facebook, Twitter and LinkedIn with SPIDER project news.	AVAILABLE: - Facebook, LinkedIn, Twitter - YouTube

More specifically, as reported in D8.2 "Initial report on dissemination, communication, standardization and exploitation" [8] and D8.3 "Interim Report on dissemination, communication, standardisation, and exploitation" [9], during the first 30 months of the project lifecycle, the various awareness activities can be grouped in the following framework:

General public dissemination

- Creation of the project website and dynamic update of its contents
- Creation of SPIDER profile in 4 social networks: Twitter, Facebook, Youtube and LinkedIn
- Creation of leaflet and brochure for SPIDER's dissemination purposes.
- Co-organizers and sponsors of the 6th Network and Information Security (NIS'19) Summer School took place in Crete, Greece during September 2019.
- Co-organizers of one joint webinar along with FORESIGHT and CYBER-MAR projects
- Co-organizers of a joint workshop along with FORESIGHT CYBER-MAR, THREAT ARREST, SPARTA, CONCORDIA etc.
- Organization of two workshops in collaboration with the CERTS /CSIRTs
- Sponsors of the Cybersecurity Hands-On-Training (CyberHOT) Summer School which took place on September 2021 in Crete, Greece, under the auspices of NMIOTC (NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE)
- Release of two project newsletters
- Leaflet, brochure, posters available at the project website
- Social media channels created and constantly updated

Scientific dissemination as far

- Accepted paper for RCIS2020 event
- Presentation of a poster for the EUCNC2020 event
- 9 conference papers acknowledging SPIDER accepted at RCIS 2020, EUCNC 2020, NETSOFT, and IEEE ICC 2020 Workshop on Convergent Internet of Things, IEEE CSR 2021, EUCNC 2021
- 6 journal papers accepted to various journals
- 1 whitepaper released

Dissemination in industry, standardization bodies and open-source community

- Participation to various national and international events for raising awareness around the project
- Involvement with industry forums and special interest groups.

4.1.1 Social Media and Website

At the very beginning of the project lifecycle the effort has been allocated to setup the website and the respective social media (Twitter/Facebook/LinkedIn/YouTube).

The SPIDER website (https://spider-h2020.eu) went live in October 2019 (M4) and is considered as the major channel of information and communication. Therefore, its structure and layout are interrelated with the main goals of disseminating the project results to the general public, experts in the field and to engage key stakeholders. A dedicated space for accessing dissemination materials such as leaflets, brochures, newsletters, videos etc. has been created. All project material (brochures, leaflets, newsletters, presentations, videos, webinars) can be found under the following link:

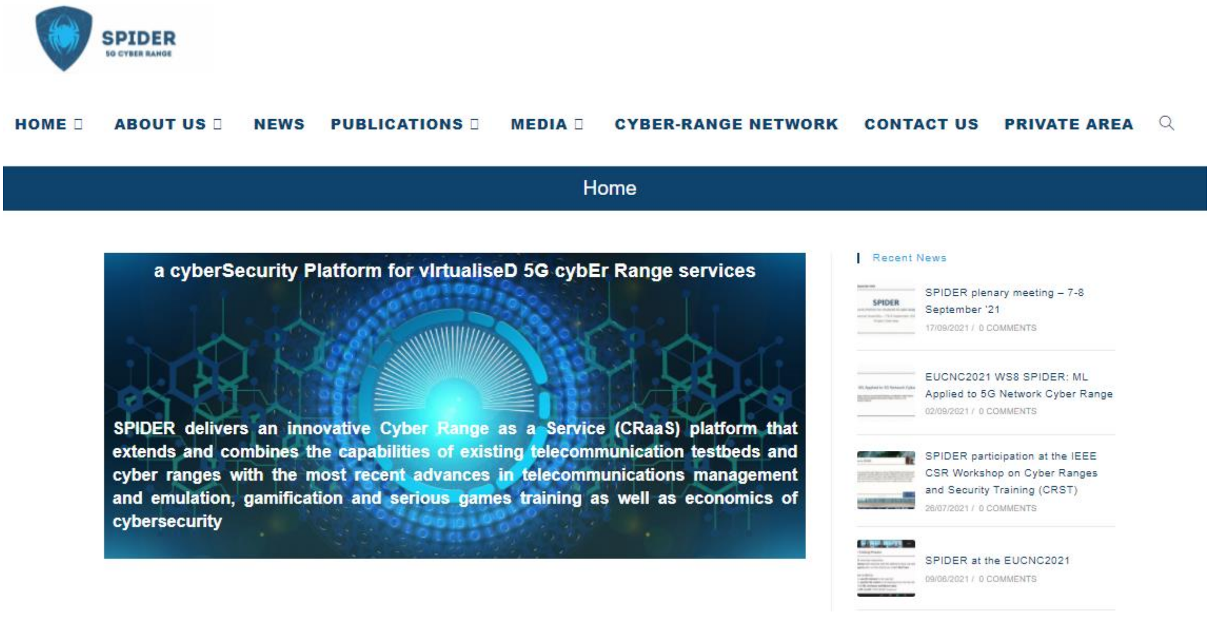
https://spider-h2020.eu/media/

All publications that acknowledge our project can be found in open mode access (Zenodo) here:

https://spider-h2020.eu/publications/#Research-Papers

The website is being updated regularly with all SPIDER updates that can be found at the following link:

https://spider-h2020.eu/news/



a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

SPIDER delivers an innovative Cyber Range as a Service (CRaaS) platform that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges with the most recent advances in telecommunications management and emulation, gamification and serious games training as well as economics of cybersecurity

Recent News

SPIDER plenary meeting – 7-8 September '21
17/09/2021 / 0 COMMENTS

EUCNC2021 WS8 SPIDER: ML Applied to 5G Network Cyber Range
02/09/2021 / 0 COMMENTS

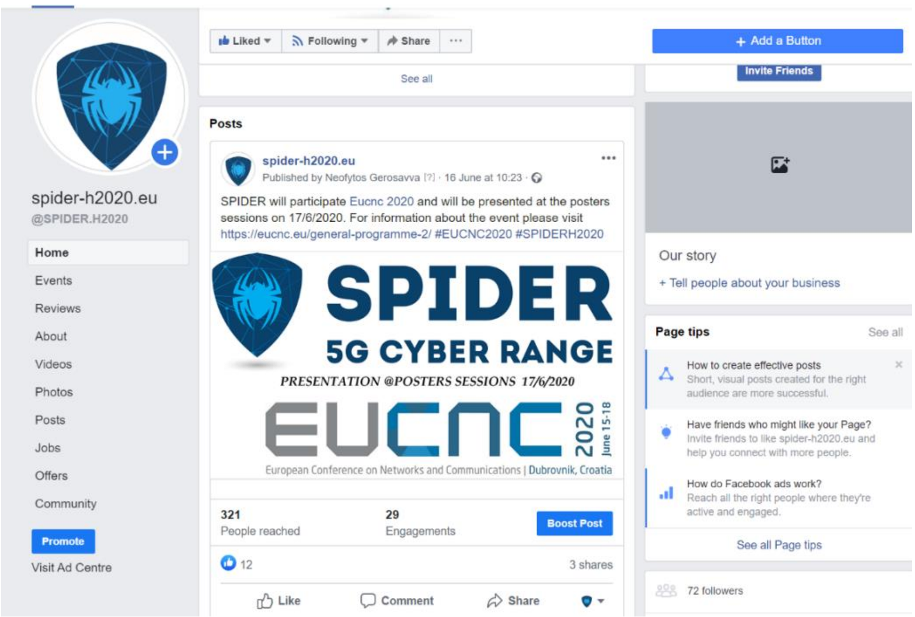
SPIDER participation at the IEEE CSR Workshop on Cyber Ranges and Security Training (CRST)
26/07/2021 / 0 COMMENTS

SPIDER at the EUCNC2021
09/06/2021 / 0 COMMENTS

Figure 2: Website homepage

Nowadays social media networks are perhaps the most popular and efficient channels to promote a project and enhance its visibility. Using social networks channels and media, it is possible to increase the reputation of SPIDER and create a "stronger stakeholders' network" among the different involved "actors" in this knowledge sharing process. During the first 3 months of the project lifecycle, project accounts were created on Facebook and Twitter. An account on LinkedIn followed on M8. Updates on the news and progress of the project are published at regular time intervals.

The SPIDER Facebook page (https://www.facebook.com/SPIDER.H2020/) provides an analytics functionality that gives a deeper insight of user activities and the impact that posts have on followers.



spider-h2020.eu
Published by Neofytos Gerosavva [?] · 16 June at 10:23

SPIDER will participate Eucnc 2020 and will be presented at the posters sessions on 17/6/2020. For information about the event please visit https://eucnc.eu/general-programme-2/ #EUCNC2020 #SPIDERH2020

321 People reached
29 Engagements
12
3 shares

How to create effective posts
Short, visual posts created for the right audience are more successful.

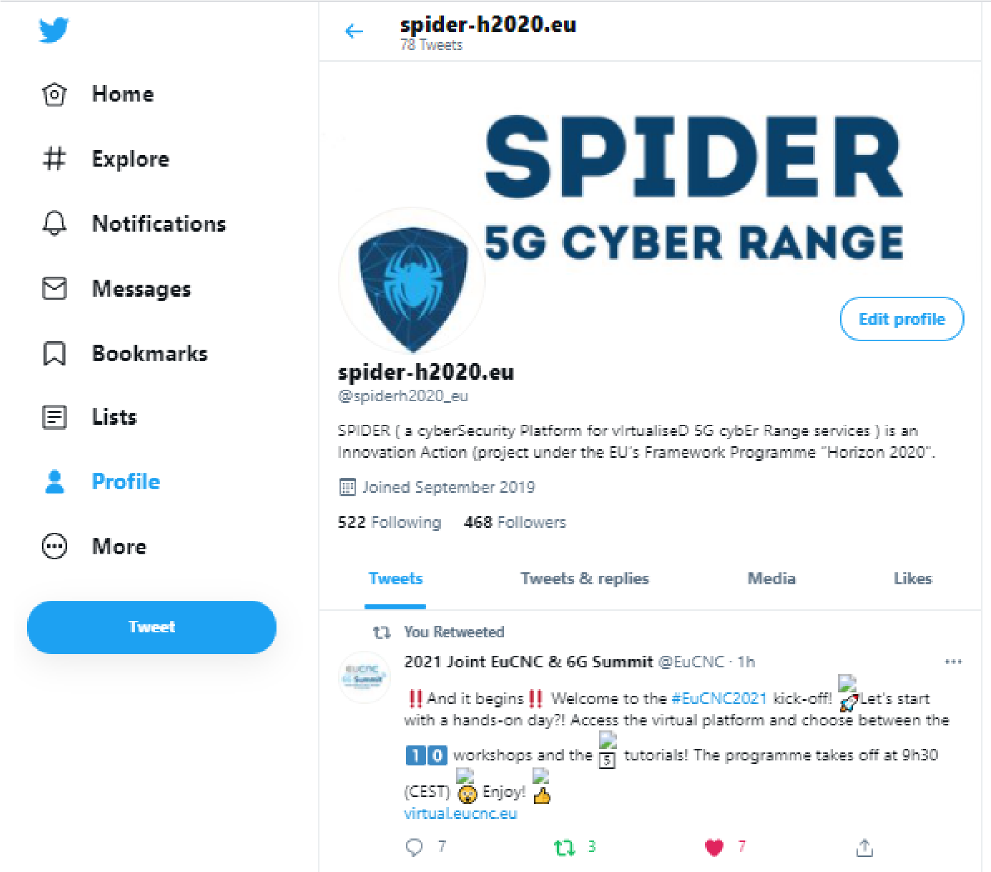
Have friends who might like your Page?
Invite friends to like spider-h2020.eu and help you connect with more people.

How do Facebook ads work?
Reach all the right people where they're active and engaged.

72 followers

Figure 3: SPIDER Facebook page

A Twitter account (https://twitter.com/spiderh2020_eu) was setup at the very beginning of the project. The Twitter account can be followed via @spiderh2020_eu.



spider-h2020.eu
78 Tweets

spider-h2020.eu
@spiderh2020_eu

SPIDER (a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services) is an Innovation Action (project under the EU's Framework Programme "Horizon 2020".

Joined September 2019

522 Following 468 Followers

You Retweeted

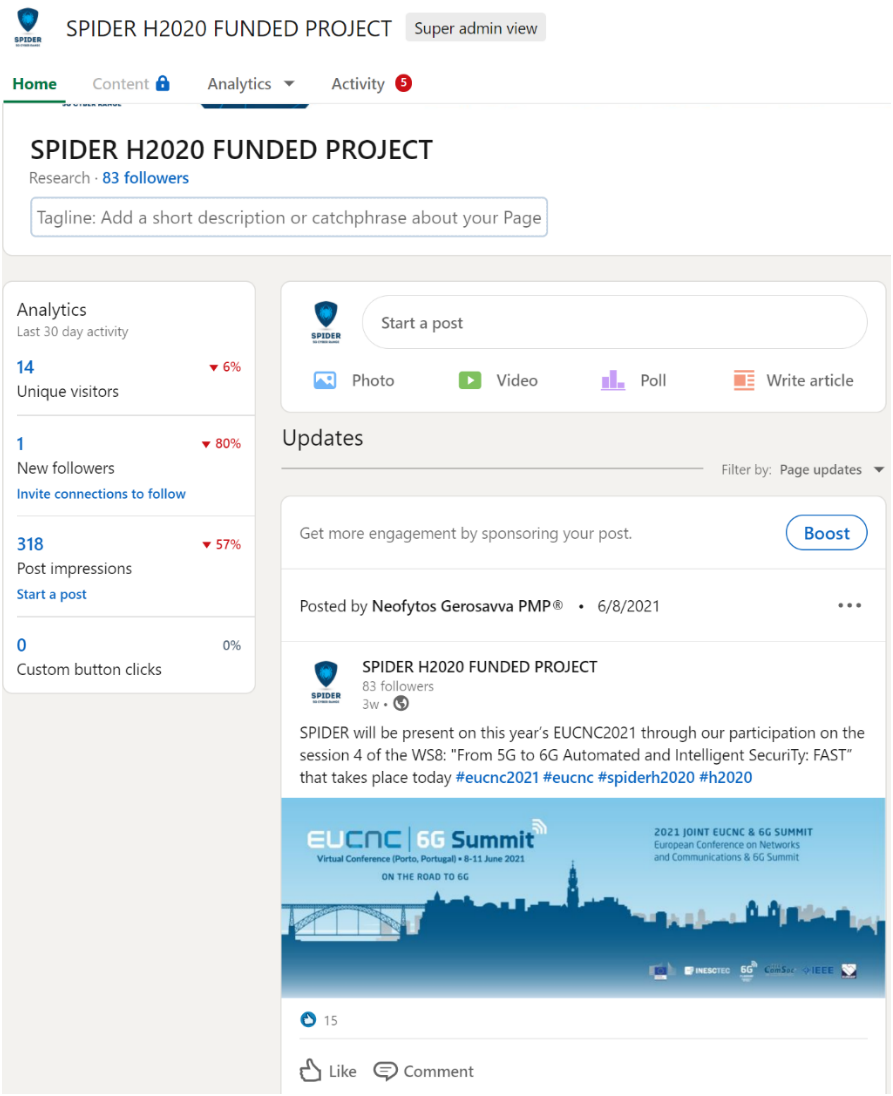
2021 Joint EuCNC & 6G Summit @EuCNC · 1h

‼️And it begins‼️ Welcome to the #EuCNC2021 kick-off! 🚀Let's start with a hands-on day?! Access the virtual platform and choose between the 1️⃣0️⃣ workshops and the 5️⃣ tutorials! The programme takes off at 9h30 (CEST) 😮 Enjoy! 👍
virtual.eucnc.eu

7 3 7

Figure 4: SPIDER Twitter page

The SPIDER LinkedIn page (https://www.linkedin.com/company/spider-h2020-funded-project/) was created last (around month 8) and, also in this case, it provides a statistics and analytics functionality that gives a deeper insight of this social media account posts' impact.


SPIDER H2020 FUNDED PROJECT Super admin view

Home Content Analytics Activity 5

SPIDER H2020 FUNDED PROJECT
Research · 83 followers
Tagline: Add a short description or catchphrase about your Page

Analytics
Last 30 day activity

14 ▼ 6%
Unique visitors

1 ▼ 80%
New followers
Invite connections to follow

318 ▼ 57%
Post impressions
Start a post

0 0%
Custom button clicks

Start a post
Photo Video Poll Write article

Updates
Filter by: Page updates

Get more engagement by sponsoring your post. Boost

Posted by Neofytos Gerosavva PMP® • 6/8/2021

SPIDER H2020 FUNDED PROJECT
83 followers
3w •

SPIDER will be present on this year's EUCNC2021 through our participation on the session 4 of the WS8: "From 5G to 6G Automated and Intelligent SecuriTy: FAST" that takes place today #eucnc2021 #eucnc #spiderh2020 #h2020

EUCNC | 6G Summit
Virtual Conference (Porto, Portugal) • 8-11 June 2021
ON THE ROAD TO 6G
2021 JOINT EUCNC & 6G SUMMIT
European Conference on Networks and Communications & 6G Summit
INESCTEC
6G
ComSoc
IEEE

15

Like Comment

Figure 5: SPIDER Linkedin account

4.1.2 Dissemination Material Representing the Project

Dissemination material, and more specifically, a leaflet and a brochure have been created to provide to the readers the SPIDER vision, objectives, approach, actors and use cases. Leaflet and brochure are designed with the projects colours and also include the project logo, the project's social media and website links, and of course proper EU acknowledgment and disclaimer, according to the Grant Agreement.

The leaflet and brochure are available for download under the following links:

https://spider-h2020.eu/wp-content/uploads/2020/03/a4_flyer.pdf https://spider-h2020.eu/wp-content/uploads/2020/03/3foldflyer.pdf

The newsletters represent a dissemination tool of the news about the project, the consortium, the main activities, and achievements performed during the lifecycle progress. The SPIDER newsletter uses the project's colour palette (blue and white) and the front page includes the project logo, a small summary, the project vision and objectives, and an acknowledgment of the European Union funding, along with the proper disclaimer. The first newsletter was released in March 2020 and can be found here:

Issue #1: https://spider-h2020.eu/wp-content/uploads/2020/03/Spider_Newsletter-FINAL.pdf

SPIDER released the second newsletter in February 2021, that includes information about the project's technical progress status, achievements, clustering, and dissemination activities. This document can be found here:

Issue #2: https://spider-h2020.eu/wp-content/uploads/2021/02/NEWSLETTER-ISSUE-2-FINAL.pdf

A third newsletter is planned to be released by the end of the December 2021

4.1.3 Activities and Events

The main dissemination activities initiated in the earlies months included participation and promotion of SPIDER overview and solution proposal carried out by various partners either physically or virtually in different kind of workshops, conferences, forums, meetings, and webinars.

The following tables provide a list of events where the SPIDER project was represented and disseminated from consortium members, sorted by project year. We must re-iterate that some activities were affected from COVID-19 pandemic, something that prevented face-to-face project promotion. This happened especially in the early phases before virtual platforms initiated to be widely adopted as the main communication channel.

Table 2 – Events participated by consortium members during the first year of the project

	EVENT NAME	PARTNER	DATE
1	ETSI SECURITY WEEK (standardization activity)	TID	19 Jun '19
2	ETSI EXPERIENTAL NETWORKED INTELLIGENCE INDUSTRY SPECIFICATION GROUP (ENI ISG) (standardization activity)	TID	9-11 Jul '19
3	6th NETWORK AND INFORMATION SECURITY (NIS'19)	FORTH	16-20 Sep '19
4	RESEARCHER'S NIGHT	FORTH	27 Sep '19
5	6th EAB. CYBER MEETING	UPRC	19 Nov '19
6	REA EVENT	ERICSSON	31 Jan '20
7	Resilience (CISaR) workshop	UPRC	30-31 Jan '20
8	Mastering Enterprise Risk Management-	UPRC	30-31 Jan '20
9	SECURITY AND CYBERSECURITY HELIX EVENT	EIGHT BELLS	5-6 Feb '20
10	SECURE INTERNET DAY	UPRC	11 Feb '20
11	THE EUROPEAN CYBER SECURITY CHALLENGE 2020	UPRC	13-14 Feb '20
12	DISCUSSION AT GREEK NATIONAL RADIO	UPRC	17 Feb '20
13	7th INFORMATION SECURITY CONFERENCE	UPRC	19 Feb '20

14	EAB CYBER MEETING IN VTC	UPRC	5 May '20
15	IEEE ICC2020 (PAPER ACKNOWLEDGING SPIDER- VIRTUAL PRESENTATION)	FBK	7-11 Jun '20
16	EUCNC2020 (PAPER ACKNOWLEDGING SPIDER – VIRTUAL PRESENTATION)	CNIT, INFOCOM	16 Jun '20
17	EUCNC 2020 (POSTER -VIRTUAL PRESENTATION)	EIGHT BELLS, UPRC, CYBERLENS, ERICSSON, TID	17 Jun '20

Table 3 – Events participated by consortium members during the 2nd year of the project

	EVENT NAME	PARTNER	DATE
1	RCIS CONFERENCE	EIGHT BELLS	22 Sep '20
2	CONCORDIA Open Door (COD) 2020	EIGHT BELLS /ALL	28-29 Oct '20
3	5G Experimentation Facilities and Vertical Trials webinar	UPRC	14 Oct '20
4	INFOCOM WORLD CONFERENCE	EIGHT BELLS	3 Nov '20
5	IEEE International Conference on Cloud Networking	TID	9-11 Nov '20
6	5G TECHRITORY forum	FORTH	11-12 Nov '20
7	IEEE CONFERENCE ON NETWORK FUNCTION VIRTUALIZATION AND SOFTWARE DEFINED NETWORKS	TID	9-12 Nov '20
8	SPIDER AT ERICSSON DGS TECHNOLOGY DAYS 2020	ERICSSON	1 Dec '20
9	SPIDER at Ericsson Virtual Technology Day Athlone 2020	ERICSSON	10 Dec '20
10	CYBERWISER.eu training event	EIGHT BELLS	25 Mar '21
11	"Territory and Infrastructure Security in the Digital Age"	INFOCOM	4 Apr '21
12	Spanish Network of Excellence on Cybersecurity Research (RENIC)	TID	20 Apr '21
13	FIWARE CYBERSECURITY DAY	EIGHT BELLS	13 May '21
14	EUCNC 2021	TID /UPM	8 Jun '21
15	2021 IEEE CSR – IEEE Conference on Cyber Security and Resilience	CO-ORGANIZERS AND PAPER BY CITY/CLS/ 8BELLS	26-28 Jul '21

Table 4 – Events participated by consortium members during M25-M29 of the project

	EVENT NAME	PARTNER	DATE
1	Cybersecurity Hands -On -Training (CyberHOT) Summer School	FORTH	27-28 Sep '21
2	Career Day: Meet the companies	STS	18 Oct '21
3	CONCORDIA OPEN DOOR 2021 as virtual exhibitors	EIGHT BELLS, SGI, TID/UPM, CLS	20-21 Oct '21
4	IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks	UPRC	25-27 Oct '21
5	SPIDER at R&D Italy Innovation Event 2021	ERICSSON	1 Dec '21

4.1.4 Papers, Journal Articles and Posters

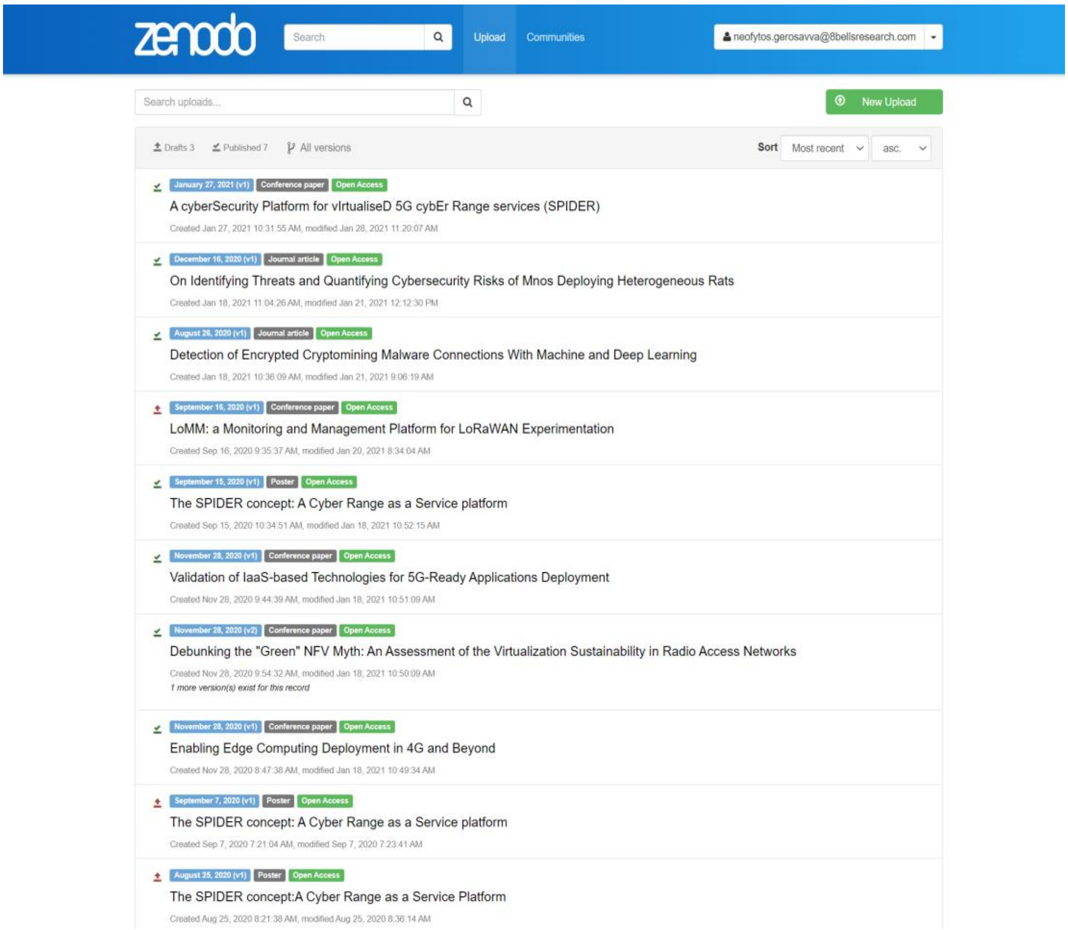
Table below (Table 5) includes all the papers that acknowledge SPIDER so far at M30. In total, 15 accepted peer-reviewed papers (9 in conferences and 6 in journals) are acknowledging the SPIDER project.

Table 5 - List of SPIDER scientific peer reviewed publications

#	Paper NAME	Journal /Conference	PARTNER
1	"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	**Conference-** 5th IEEE ICC 2020 Workshop on Convergent Internet of Things	FBK
2	"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	**Conference –** EUCNC 2020	CNIT /INFOCOM/ ATOS
3	"Debunking the "Green" NFV Myth: An Assessment of the Virtualization Sustainability in Radio Access Networks"	**Conference-** NetSoft 2020	CNIT
4	"Enabling Edge Computing Deployment in 4G and Beyond"	**Conference-** NetSoft 2020	CNIT /INFOCOM
5	"Acceleration of Intrusion Detection in Encrypted Network Traffic Using Heterogeneous Hardware"	**Journal-** Sensors 2021	FORTH
6	"On identifying threats and quantifying cybersecurity risks of MNOs deploying heterogeneous RATs"	**Journal-** IEEE-Access	UPRC
7	"NodeXP: NOde.js server-side JavaScript injection vulnerability DEtection and eXPloitation"	**Journal-** Information Security and Applications	UPRC
8	"Dynamics of Fourier Modes in Torus Generative Adversarial Networks"	**Journal-** Open access "Mathematics"	UPM
9	"Detection of encrypted cryptomining malware connections with machine and deep learning"	**Journal-** IEEE-Access	UPM/ TID
10	"[m]allotROPism: A Metamorphic Engine for Malicious Software Variation Development" International Journal of Information Security, Springer	**Journal-** **"**International Journal of Information Security, Springer" -IJIS journal	UPRC
11	"The SPIDER Concept: A Cyber Range as a service platform"	**Conference-** EUCNC2020	EIGHT BELLS, CLS, UPRC, ERICSSON, TID
12	"A cyberSecurity Platform for vIrtualiseD 5G cybEr Range services (SPIDER)"	**Conference-** RCIS2020	EIGHT BELLS, CLS, FORTH, UPRC, ERICSSON
13	"The SPIDER Cyber Security Investment Component (CIC)"	**Conference-** 2021 IEEE International Conference on Cyber security and Resilience	CITY, CLS, EIGHT BELLS
14	"SPIDER: ML Applied to 5G Network Cyber Range"	**Conference-** EUCNC 2021	TID /UPM
15	"A Digital Twin Network for Security Training in 5G Industrial Environments"	**Conference-** IEEE International Conference on Digital Twins and Parallel Intelligence.	TID /UPM

4.1.5 Papers -Open Access

SPIDER uses Zenodo as the platform for storing and managing the data generated and OpenAIRE for linking the databases and publications. Thus, we have indexed most of our papers in Zenodo and OpenAIRE (Figure 6) according to EU guidelines and they are available for downloading and reading in our website: https://spider-h2020.eu/publications/#Research-Papers



January 27, 2021 (v1) Conference paper Open Access
A cyberSecurity Platform for vIrtualiseD 5G cybEr Range services (SPIDER)
Created Jan 27, 2021 10:31:55 AM, modified Jan 28, 2021 11:20:07 AM

December 16, 2020 (v1) Journal article Open Access
On Identifying Threats and Quantifying Cybersecurity Risks of Mnos Deploying Heterogeneous Rats
Created Jan 18, 2021 11:04:26 AM, modified Jan 21, 2021 12:12:30 PM

August 26, 2020 (v1) Journal article Open Access
Detection of Encrypted Cryptomining Malware Connections With Machine and Deep Learning
Created Jan 18, 2021 10:36:09 AM, modified Jan 21, 2021 9:06:19 AM

September 16, 2020 (v1) Conference paper Open Access
LoMM: a Monitoring and Management Platform for LoRaWAN Experimentation
Created Sep 16, 2020 9:35:37 AM, modified Jan 20, 2021 8:34:04 AM

September 15, 2020 (v1) Poster Open Access
The SPIDER concept: A Cyber Range as a Service platform
Created Sep 15, 2020 10:34:51 AM, modified Jan 18, 2021 10:52:15 AM

November 28, 2020 (v1) Conference paper Open Access
Validation of IaaS-based Technologies for 5G-Ready Applications Deployment
Created Nov 28, 2020 9:44:39 AM, modified Jan 18, 2021 10:51:09 AM

November 28, 2020 (v2) Conference paper Open Access
Debunking the "Green" NFV Myth: An Assessment of the Virtualization Sustainability in Radio Access Networks
Created Nov 28, 2020 9:54:32 AM, modified Jan 18, 2021 10:50:09 AM
1 more version(s) exist for this record

November 28, 2020 (v1) Conference paper Open Access
Enabling Edge Computing Deployment in 4G and Beyond
Created Nov 28, 2020 8:47:38 AM, modified Jan 18, 2021 10:49:34 AM

September 7, 2020 (v1) Poster Open Access
The SPIDER concept: A Cyber Range as a Service platform
Created Sep 7, 2020 7:21:04 AM, modified Sep 7, 2020 7:23:41 AM

August 25, 2020 (v1) Poster Open Access
The SPIDER concept:A Cyber Range as a Service Platform
Created Aug 25, 2020 8:21:38 AM, modified Aug 25, 2020 8:36:14 AM

Figure 6: SPIDER publications available in open access on the Zenodo website

4.1.6 SPIDER Whitepaper

The project produced a first whitepaper to provide an insight on the SPIDER requirement capturing along with architecture componentization and use case definition during the first half of the project. More specifically, this document focused on presenting the activities on WP2 “Requirements Analysis, Architecture Definition and Pilot Use Cases”, and the main outcomes of the relevant deliverables produced in the timeframe. This paper was released in January ’20 and was authored by several consortium members.

The paper can be accessed here: https://spider-h2020.eu/wp-content/uploads/2021/01/SPIDER---WHITEPAPER-1.pdf

A second whitepaper is planned for the end of project (M36) according to the Dissemination plan. This second whitepaper will present the final technical solution of the project. It will be published on the SPIDER website and will be promoted through all project's social media.

4.1.7 Other Activities

CYBER RANGE Network

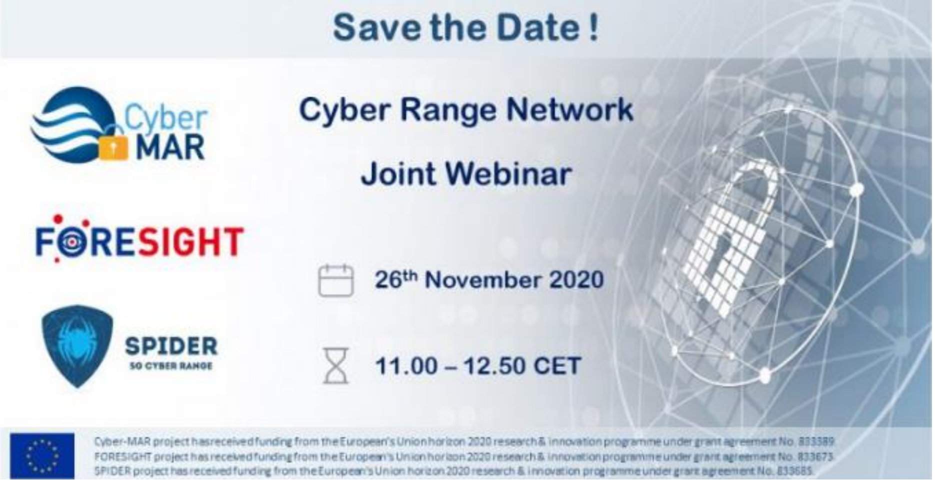
A specific initiative has been undertaken regarding clustering activities that SPIDER project formulated along two other H2020 projects, namely FORESIGHT and CYBER-MAR projects. The clustering has been "branded" as the "Cyber-Range network" with a main purpose to make widely known projects results, raise awareness on cybersecurity and promote the use of cyber ranges.

Figure 7: The CYBER RANGE Network

All the relevant information can be found here: https://spider-h2020.eu/cyber-range-network/

CYBER-RANGE NETWORK webinar

Towards this direction the three projects organized a joint CYBER-RANGE NETWORK webinar that took place on November 26, 2020.


Cyber
MAR
FORESIGHT
SPIDER
5G CYBER RANGE

Save the Date !

Cyber Range Network

Joint Webinar

26th November 2020

11.00 – 12.50 CET

Cyber-MAR project hasreceived funding from the European's Union horizon 2020 research & innovation programme under grant agreement No. 833389
FORESIGHT project has received funding from the European's Union horizon 2020 research & innovation programme under grant agreement No. 833673
SPIDER project has received funding from the European's Union horizon 2020 research & innovation programme under grant agreement No. 833685

Figure 8: The registration form of the joint webinar

The format included deployment of various presentations shared by the three projects representatives offering a comprehensive description of their project current activities. The joint webinar can be found at our YouTube channel here:

https://www.youtube.com/watch?v=Yjx0TdwivnQ

2021 IEEE CSR WORKSHOP ON CYBER-RANGES AND SECURITY TRAINING (CRST)

The collaboration has continued through organization of additional events and other activities. A proposal has been submitted along FORESIGHT, CYBER-MAR and other projects for organizing a joint workshop in July 2021. The proposal has been accepted under the name "Cyber Ranges and Security Training (CRST)" by IEEE CSR 2021. The initiative concretized in SPIDER being the co-organizer and supporter along with other friend projects such as CYBER-MAR, FORESIGHT, THREAT-ARREST, CONCORDIA, SPARTA etc. of the 2021 IEEE CSR Workshop on Cyber Ranges and Security Training (CRST).

The workshop took place on July 26, 2021. All the relevant information about this event can be found here: https://www.ieee-csr.org/workshops/crst/

CRST 2021
2021 IEEE CSR Workshop on Cyber Ranges and Security Training (CRST)
FORESIGHT
Cyber MAR
SPIDER
THREAT ARREST
ECHO
CONCORDIA
Cyber Security for Europe
SPARTA

Figure 9: The CRST workshop logo and supporting projects

Workshop with EU CERTs/CSIRTs

The 1st SPIDER 5G Cyber Range workshop for EU CERT/CSIRTs took place virtually on 21 April, 2021, and was attended by more than 20 participants. Among the participants were representatives from organizations such as BU-CERT, CYPRUS NATIONAL CSIRT, HELLENIC CSIRT and the GR.NET CERT. This event's aim was to establish operational connections with CERTs/CSIRTs, discuss, interchange information, present SPIDER's tools and training material and receive feedback on the current technical status of the project. In the scope of this workshop were presented various topics from the project, such as a generic overview of SPIDER and its objectives, SPIDER Architecture as a Cyber Range Service Platform, SPIDER Modalities and Pilot Use Cases, and SPIDER's Cyber Risk Analysis Methods and Econometric Models. Furthermore, a live demo of the SPIDER Platform was presented demonstrating the current status and the various functionalities of the SPIDER platform. Finally, the

SPIDER consortium had the opportunity to answer questions regarding the platform and exchange opinions with the participants towards common interests and aims.

The 2nd SPIDER 5G Cyber Range workshop for EU CERT/CSIRTs took place virtually on 13 May, 2021, and was attended by 16 participants. Among the participants were representatives from organizations such as BU-CERT, CYPRUS NATIONAL CSIRT, HELLENIC CSIRT and the GR.NET CERT. This meeting was the continuation of the first workshop offering the chance to present other important project aspects, such as Continuous Risk Analysis within SPIDER and the Continuous Risk Analysis Engine (CRAE) engine, the SPIDER Cybersecurity Investment Component and finally SPIDER's potential offerings to the liaised CERTs and next steps workshop with the CERTs. The established link s aimed to remain active until the end of the project, providing the SPIDER's technical offerings and training material to the CSIRT/CERTs community, receiving feedback that will assist the exploitation of the platform to more sectors that prior envisioned.

Figure 10: CERTs/ CSIRTs that have attended the 2 workshops

Presentation to the CONCORDIA consortium and joining the CONCORDIA's Observer Stakeholder Group

Additionally, the project delivered a presentation to the CONCORDIA consortium during September 2020, and initiated discussion on possible synergies and ways to disseminate jointly our project results. Towards this direction, SPIDER joined also 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. For more information about the OSG please visit: https://www.concordia-h2020.eu/concordia-service-community-pact/

Figure 11: CONCORDIA logo

Horizon Results Booster services

Furthermore, SPIDER and CONCORDIA have been working together to enhance dissemination and communications activities with the use of the services of Horizon Results Booster. In particular, SPIDER, as member of the CONCORDIA Project Group on Horizon Results Booster platform, made use of SERVICE 1 “Portfolio Dissemination and Exploitation Strategy (PDES)”, MODULE A: Identification and creation of the portfolio of R&I project results. The related outcome of this service, namely “Portfolio of Research and Innovation Results Project Group: CONCORDIA 830927” has been finalised and made available to all projects on December 1st 2021.

Supported by the European Commission’s HRB programme, CONCORDIA, SPIDER and FORESIGHT have taken the first step towards forming a Project Group based on commonalities between their work in the field of cyber ranges. HRB supports the effective transfer of research and innovation project results to policymakers, industry and society by offering various services as dissemination, exploitation strategy and business plan development to projects supported under the 7th Framework Programme (FP7) or Horizon 2020 funding schemes.

4.2 MARKET ANALYSIS AND EXPLOITATION

A preliminary market analysis report was produced within the first 12 months regarding **5G**, **cyber security, cyber range,** and **cyber awareness training** markets. Furthermore, as a result of an internal analysis, the consortium identified a preliminary number of exploitable outputs with the purpose to establish the basis for the potential of the project's outcomes. Six innovations have been identified at the end of the first 12 months. These outputs cover the SPIDER platform in general (#1), which was identified as the main item of extensive Business modelling and planning in the second half of the project. Moreover, individual submissions highlighted the innovation potential in security training, advanced cybersecurity tools, traffic emulation, and cyber risk analysis and evaluation. These, together with the new outputs identified during the second half of the project, will represent the basis for the individual and joint exploitation of the project. The SPIDER consortium at the end of M24 identified, described, and analysed 7 technical items that are part of the platform, and that represent important exploitation assets:

- **SPIDER Cyber range as a whole** (owner: SPIDER consortium);
- **5G-specific emulated Scenarios** (owner: THALES);
- **Cyber Security Serious Game** (owner: SGI);
- **ML Emulation Lab** (owners: TID/UPM);
- **XL-SIEM** (owner: ATOS);
- **Continuous Risk Assessment Engine** (owner: ATOS);
- **Assurance Platform Event Captors** (owner: STS).

The **exploitation analysis** carried out for each asset has provided an overview of its specific market positioning, the expected TRL, the licensing scheme, the analysis of the market including the existing competitors and the potential customers; an analysis of the type of exploitation foreseen both during the project execution and in the post project phase. A series of planned/desirable actions to improve the exploitation have been surveyed.

Moreover, the first version of the **market analysis** has been provided for the SPIDER Cyber Range at M24 The market analysis is composed of the following parts:

1) Cyber security requirements of the 5G;

2) Existing and possible cyber threats of the 5G; 3) 5G stakeholders;

4) The cost of cyber-attacks;

5) The expected benefits of Cyber ranges;

6) The regulatory framework and compliance;

7) The analysis of the competition;

8) the market outlook on cyber security, cyber security training and education, 5G, and cyber insurance.

This analysis will serve as the basis for developing the business plan and the economic analysis of the project in the final project period.

4.3 STANDARDIZATION

The dedicated task is monitoring standardization bodies and open initiatives identified at the beginning of the project.

Initially SPIDER was represented at two standardization workshops:

- **ETSI SECURITY WEEK (June 2019 at Sophia Antipolis, France)**

- **ETSI EXPERIENTIAL NETWORKED INTELLIGENCE INDUSTRY SPECIFICATION GROUP (ENI ISG)/ ETSI SECURITY WEEK (July 2019 at Aveiro, Portugal)**

Subsequently, the standardization activities have progressed over line of actions that were already in place and during the advancement of research within SPIDER, mainly addressing ETSI which is recognised as a European Standards Organisation and IETF/IRTF bodies which are both working in research issues in protocol and applications.

The activity at the timing of writing this report, i.e. M30 (Dec '21), can be summarized as follows:

- Finalised the contribution to the published ETSI ENI whitepaper ***"ENI vision: Improved network experience through Experiential Networked Intelligence"*** ***(***https://www.etsi.org/images/files/ETSIWhitePapers/etsi-wp44_ENI_Vision.pdf***)***. This white paper defines a common AI/ML framework into network management, with use cases and proofs-of-concept applying AI-based tools in security and 5G. Some attacks from the SPIDER use case were reflected in this whitepaper. The document was published in March 2021.
- Leverage the opportunity to contribute to the SPIDER Edge related use case in the published ETSI MEC whitepaper ***"MEC security: Status of standards support and future evolutions"*** ***(***https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_WP_46-_MEC_security.pdf***)***. This white paper introduces threats and potential attacks against MEC infrastructure and information contained. The document was published in May 2021.
- Bring the concept of Networks Digital Twin (NDT), (a.k.a. Mouseworld) for AI/ML tools creation used in SPIDER on published ***ETSI GR ENI 010*** applicability categorisation document (https://www.etsi.org/deliver/etsi_gr/ENI/001_099/010/01.01.01_60/gr_ENI010v010101p.pdf). The standard was published in March 2021.

Also, other standardisation activities have progressed over the already started line of actions:

- Consolidated draft on the ***IETF DTN (Digital Twin Network) concept*** (https://tools.ietf.org/html/draft-zhou-nmrg-digitaltwin-network-concepts-05) in the IRTF NMRG working group. This draft was initiated in the previous project period and added SPIDER key concepts: Network (twin) Orchestrator for AI and cyber-training. The draft progresses well over several iterations and in several IETF 109-111 meetings, with explicit reference to the SPIDER project in the actual draft.
- Active participation in the ***ongoing working-item ETSI SAI-003, "Security Testing of AI"***, analysing opportunities related to adversarial network applicability, as developed in SPIDER.
- Monitoring open-source opportunities to contribute such as free5G, open5gs and OSM.

4.4 Liaison with Stakeholders and Creation of Operational Links with EU CERTs/CSIRTs

As part of the awareness framework a methodology and initial plan for the liaison activities with the EU CERTs/CSIRTs and other stakeholders has been developed, among which the list of EU CERTs of ENISA have been extracted. In the initial report on connections with stakeholders and European CERTs/CSIRTs it has been described the work plan, material and communication activities that were pursued during the first reporting period of the project (M1-M18), as well as the means used to accomplish the objectives set for this project timeframe, i.e. D8.6 “Report on connections with stakeholders and European CERTs/CSIRTs - initial version” [10].

The initiative undertaken started with engagement phase sending invitations to CERTs/ CSIRTs and receiving acceptance from:

- Hellenic CSIRT
- GRNET CERT
- Cyprus National CERT
- Bournemouth University BU CERT

During April – May 2021, a two stages workshop has been organized with the accepted CERT/CSIRTs, where we presented all SPIDER offerings, the needs of the CERT/CSIRT’s community and how SPIDER can serve these needs. We also provided all dissemination material to them and received their commitment to assist us by providing feedback through questionnaires or during workshops.

Liaising activities with other projects include meetings with CONCORDIA and THREAT ARREST to deliver training cyber-range models. In addition, a number of 5G projects have agreed on participating in SPIDER events and hands-on workshops. This will further enhance the feedback for the final SPIDER evaluation.

4.5 Deliverables of the Awareness Framework

Finally, the project activities have been reported according to the following deliverables:

D8.1 Plans for dissemination, communication, standardization and exploitation [7]

This document describes how the SPIDER consortium can establish and follow highly effective dissemination and communication activities to promote the project and record how the results are being exploited.

D8.2 Initial report on dissemination, communication, standardization and exploitation [8]

It describes the dissemination, and communication activities that were pursued during the first year of the project (M1-M12), including also information related to standardization and exploitation activities. Details are given for the participation to the various conference events, the communication initiatives, the scientific paper publications, the progress on standardisation, the market analysis to outline the exploitation strategy and the methodology and initial plan for the liaison activities.

D8.3 Interim report on dissemination, communication, standardisation and exploitation [9]

This document represents the Interim report on dissemination, communication, standardisation and exploitation updated after 24 months concerning the initiative undertaken to raise awareness around project’s outcomes and promote the project results through various channels. These channels could refer to scientific publications, journal articles, posters, presentation at workshops and conferences, webinars, training courses, events participation etc. It also reports on advancement related to standardization and exploitation activities, including market outlook and analysis of the competitors.

D8.6 Report on connections with stakeholders and European CERTs/CSIRTs - initial version [10]

It is the initial version of the report concerning the liaison activities undertaken by the project, describing the work plan, material and communication activities that were pursued during the first reporting period of the project (M1-M18). The deliverable describes in detail all the rationale behind all completed and planned activities as well as the results of the liaison activities at the time of this reporting.

Furthermore, by the end of the project, the following reports are foreseen to draw the conclusions after the foreseen 36months of activities:

D8.4: Final report on dissemination, communication, standardisation and exploitation, which will document all dissemination, communication and standardisation activities in the second half of the project.

D8.5: Market analysis, roadmapping and business modelling report, which will be an internal report only, subject to confidentiality restrictions.

D8.7: Report on connections with stakeholders and European CERTs/CSIRTs – final version, final version of the report on the progress and work of the related task.

5 SPIDER Practical and Social Implications

5.1 Practical Implications

The goal of SPIDER is to implement a novel 5G cyber-range platform which targets 5G networks. A 5G deployment incorporates sophisticated programmable infrastructure that requires end to end programmability, i.e., programmability that spans from the backhaul part of the network to the radio part.

As specified in D6.2 “First integrated SPIDER platform prototype” [5], the outcome of SPIDER is aimed to assist security professionals of various levels (expert, intermediate, and novice) to leverage their skills by **conducting exercises in realistic environments that emulate real deployments**, by **automating as much as possible the performance tracking of trainees** and the **extraction of their learning gaps**, by **providing self-paced educational material regarding theoretical aspects of security** and by **providing a simulation environment where trainees can experiment with several mitigation and econometric models**.

From this perspective, the value proposition of SPIDER outcome is centred into four distinct modalities; namely i) **theoretical training**, ii) **emulation (or hands-on training)**, iii) **simulation through a serious game** and iv) **Security-awareness training.** Each of these modalities corresponds to different type of end-users. All in all, the entire platform incorporates many roles.

These roles include: **a) Training Scenario Creator** (**TSC**) that is responsible for creating emulation and simulation scenarios; **b) Training Scenario Supervisor** (**TSS**) that is responsible for initiating scenarios for specific trainees; **c) 5G Infrastructure Administrator** (**5GIA**) that is responsible for managing the 5G infrastructure; **d) Red Team Member (RTM)**that aims to attack an emulated service instance; **e)** a **Blue Team Member (BTM)** that aims to defend an emulated service and **f)** a **Non-expert cyber security trainee (NECST)** that aims to use self-paced simulation environment.

Once clarified the roles of the end-users and before elaborating more on the technical innovative capabilities of the platform, it is worth to give a view of the practical implication of positioning SPIDER into the 5G ecosystem. On this purpose, we can refer to the technology aspects of modern 5G networks that rely heavily on virtualization technology. Such technology allows agile service deployment and the promotion of the “slicing” concept which is one of the focal concepts in 5G standardization fora (3GPP, ETSI, NGMN, etc.). However, in terms of security, the leading edge turns out to be a bleeding edge. The widespread use of virtualization radically increases the attack vectors that are exposed by 5G deployments. These attack vectors can be combined by hackers to manipulate part of the infrastructure. However, the **specificities of the 5G environment** are such (usage of NFVOs, SDN switches, SDRs) **that prevents the chance of a holistic training experience for a trainee**.

SPIDER aims to tangibly cover this gap through the development of an innovative platform which has clear **feature value propositions** that include:

- the ability to **conduct exercises in a realistic environment that emulate real 5G deployments** where all 5G-integral components are present. Such environment can be parameterized and spawned on-demand. Each environment encompasses specific configuration for slice capabilities, switches, radio etc.
- the ability to **automatically infer performance tracking of trainees** and the **extraction of their learning gaps.** Emphasis is given in the “passive” tracking of trainee activities (i.e., no human

in the loop). Such inference can be used by existing models to identify the learning gaps that need to be covered.

- the ability to **provide self-paced learning regarding theoretical aspects of security through serious games**. As it is easily inferred, self-paced learning refers to simulated courses that complement the hands-on experience.
- the **provision of a simulation environment where trainees can experiment with several mitigation models on hypothetical deployments.** Such models incorporate **econometric analysis features**.

5.1.1 Feature value proposition based on learning modalities

The feature value proposition as just summarized is deployed through the following distinct learning modalities that are supported by the SPIDER platform:

- **Modality 1 – Theoretical Training**: It is the type of interaction according to which the trainee is served with a set of **theoretical/comprehension questions** (on a specific 5G sub-domain of security) to assess his/her theoretical skills.
- **Modality 2 - Emulation Training**: It is the type of interaction according to which the trainee(s) are asked to i**nteract physically** with a target deployed by SPIDER, with the goal of hacking it (for red teams) or defending it (for blue teams).
- **Modality 3 - Simulation Training through a Serious Game**: It is the type of interaction according to which trainees **calculate risks and evaluate countermeasures on top of hypothetical deployment** of interconnected vulnerable assets with the endmost goal of minimising risk subject to specific cost and resources.
- **Modality 4 - Security Awareness Training through Gamification**: It is the type of training targeting non-expert users that aim to acquire some **fundamental technical skills** that are essential in the security domain (e.g., password strengths, usage of encrypted tunnels).

With the purpose to give a high level technical overview of the SPIDER platform it is important to denote how it relies on a reference architecture that consists of a **proper componentization** along **with proper interaction and dependency tracking** among these components. The identified components are derived from the functional requirements that have been elaborate to specify the capabilities and features. A logical group has been derived into **6 environments** that represent an aggregation of components each one addressing a group of functional requirements. These environments include: **a) Emulation** environment; **b) Programmable 5G** infrastructure; **c) CV-SOC** environment**; d) Machine Learning** Lab **e) Simulation** Environment and **f) Operational Dashboards**.

5.1.2 Architecture walkthrough & SPIDER Actors

The usage of the various components is driven by functional flows that represent the functional purpose of each component and how those components interact according to the specificities of each learning modality. Important to denote that such functional flows are centred into the actors and their roles on which the users of the SPIDER platform have been grouped. Table 6 below summarizes the identified roles.

Table 6 - SPIDER Actors

Actor	Description
5G Infrastructure Administrator (5GIA)	The person who is responsible for managing the 5G infrastructure which serves as the basis for the Cyber Range platform
Training Scenario Creator (TSC)	The person responsible for creating the attack/defence scenarios and performing the corresponding system configurations
Training Scenario Supervisor (TSS)	The person responsible for managing a Training Scenario Instance (game) on top of the 5G infrastructure
Red Team Member (RTM)	Any actor who belongs in the Red team and aims to attack the 5G infrastructure
Blue Team Member (BTM)	Any actor who belongs in the blue team and aims to defend the 5G infrastructure
Non-expert cyber security trainee (NECST)	The trainee who is non-expert in cybersecurity issues

5.2 Pilot Use cases

The integrated and fully functional platform available since M24 and continuously enriched during the progress of the project in the last stages of the project is used to validate the SPIDER pilot use cases and evaluate the overall impact of the SPIDER solution and its components. SPIDER delivers three operational pilots, according to WP2 deliverables D2.5 "SPIDER user requirements and the 5G cybersecurity threat landscape – final version" [2] and D2.8 "SPIDER use cases and pilots definition – final version" [3]:

- **PUC1: Cybersecurity Testing**
- **PUC2: 5G Security Training**
- **PUC3: Cybersecurity Investment Decision Support**

Where PUC1 and PUC2 are split in more specific sub-cases, namely PUC1.a/b and PCU2.a/b, as described here below in the respective sub-sections.

5.2.1 PUC1: Cybersecurity Testing

5.2.1.1 PUC1.a: Cybersecurity Testing of 5G-ready applications and network services

The first use case focuses on representing the end-to-end services for the overall lifecycle and orchestration of 5G ready applications and network services. The goal is **to validate SPIDER in terms of its ability to support testing, performance evaluation and security assessments** of new security technologies, with emphasis on the emulation of network-wide attacks, from rudimentary to highly complex ones.

The SPIDER Cyber Range platform leverage **fully emulated 4G/5G network environments** to support PUC1.a (and PUC2.a) scenarios, guaranteeing highly reliable evaluations (and exercises) without the risks of adverse impacts on actual networks or proprietary data loss. In more detail, an emulation scenario is a 4G/5G network environment that consists of a combination of assets – such as User Equipment (UE) or UE emulators, vertical application components, physical/virtual network functions

(P/VNFs), Virtual Infrastructure Managers (VIMs), VIM tenant spaces, and Wide-area SDN Controllers (WSCs), generating an attack surface that spans from the access to the core part of the infrastructure.

PUC1.a is built on the outcomes of the **H2020 5G-PPP MATILDA project** (www.matilda-5g.eu), which has designed and developed an integrated orchestration framework for both vertical applications and network services over 5G network sliced infrastructures. The SPIDER emulation scenario components (both at application and network level) are deployed on the MATILDA infrastructure under the control of two interworking orchestration engines: (i) the **Vertical Application Orchestrator (VAO)**, which is in-charge with the network slice negotiation, as well as the deployment and decommissioning of the (geo-distributed) application components; (ii) the **Operations Support System (OSS)**, which is in-charge with the slice network creation, including the coordination of all the other building blocks in the network layer control platform – namely, the multi-site NFV Orchestrator (NFVO), Virtual Infrastructure Managers (VIMs), Wide-area Infrastructure Manager (WIM) – to set up and to properly configure base 4G/5G network services (NSs), edge computing resources, and wide-area connectivity. Furthermore, SPIDER embeds tracing capabilities into the MATILDA framework to monitor the status of assets involved in the executed test scenarios.

5.2.1.2 PUC1.b: Cybersecurity of Next Generation Mobile Core SBA

3GPP is defining the Next Generation Core (NGC) in 5G mobile networks. This NGC applies **Service Based Architecture (SBA)** and **Service Base Interfaces (SBI)**, defining a much more open relationship among the different control plane (NGC-CP) functions. This new architecture defines SBI as Web based REST API interfaces both for the internal and external NGC-CP. In addition, HTTP2 has been selected as the transport protocol for SBA, and therefore TLS (Transport Layer Security) encryption will be used by default. Current cybersecurity network tools will be stressed in this environment. An extended threat surface is expected in 5G because of this design, from lack of visibility (encrypted traffic) to new attacks applying existing tools (currently exploiting web service and application environments). PUC1.b aims at **testing and evaluating this new paradigm in SBA from the current security procedures** based on fixed reference points connecting them in a rigid, predefined schema, to a very dynamic environment of REST API interfaces and different type of encrypted traffic over TLS.

Over the variety of potential scenarios that affects encrypted traffic over TLS, SPIDER PUC1.b has selected some that can be considered as representative ones, to demonstrate how cybersecurity experts need to be prepared for new attack vectors in 5G infrastructure.

The ML Toolboxes of each scenario are going to have some pre-trained models. There are different pre-trained models because some of them are going to be faster, more precise or will provide explainable results. Also, it is going to be possible to re-train these models.

It is worth noting that the generation of attacker traffic will be also addressed in this use case researching and applying a complementary and innovative technique based on the recently appeared **Generative Adversarial Networks (GANs)**. GANs emerged in 2014 as a type of deep neural network architecture utilised to solve unsupervised learning problems in the Computer Vision area.

5.2.2 PUC2: 5G Security Training

5.2.2.1 PUC2.a: 5G Security Training for Experts

The PUC2.a scenarios are used to assess the cyber range's training capabilities for **equipping cybersecurity professionals (both individuals and teams) with 5G security skills** essential for protecting the extremely high-performance, multi-tenant and virtualized telecommunications infrastructure from both old and new threats. PUC2.a training exercises include **team-based exercises** (i.e., attack, defend and force-on-force scenarios), and **self-paced exercises** (i.e., attack and defend scenarios). Moreover, **Blue** (defence) and **Red** (attack) team exercises are implemented and tested as there are educational gaps in the existing platforms in this area (i.e., Red vs Blue teams).

Fully emulated 4G/5G network environments are exploited to implement the training scenarios. Each asset involved can contain some vulnerabilities (either inherent system properties tagged according to the Common Vulnerability Enumeration (CVE) system, or "deliberate misconfigurations") that can be exploited for an attack, or for privilege escalation and pivoting in an attack path. Moreover, each emulation scenario can be associated with several learning objectives (i.e., attack/defence actions) for the cybersecurity experts' training, such that relevant infrastructure assets and users' (Red/Blue teams) actions are monitored for tracking the training progress and performance. Monitored assets include both application- and network-level scenario components (e.g., vertical application components, P/VNFs, UEs), as well as a subset of the control platform, such as the VIM and WIM blocks.

A variety of attack scenarios that cover the training requirements for the experts and non-expert users of SPIDER platform have been defined. In the second reporting period, the emulation of some 5G-specific attacks has been added to achieve a more critical mass of representative scenarios. Hence, six (6) scenarios specific for 4G/5G threats have been deliberately defined for this purpose and included in the execution strategy of validation demonstrators.

5.2.2.2 PUC2b: 5G Security Training for Non-Experts

It has long been accepted in the security industry that experts and technical security measures cannot on their own fully protect organisations against cyber threats. The users also play a very important role, not only because they are routinely targeted by social engineering attacks, but also because proper cyber hygiene and responsible behaviour in cyber space can help detect and prevent threats. Here, the focus is not on the experts, but on the regular employees of modern network-oriented companies that need to **improve their awareness about security threat and solutions** and are trained on cutting edge technologies and the evolving 5G cybersecurity landscape. The goal is to validate that SPIDER 5G security gamification approach results in real change and provide input to the exploitation of the solution after the project end. Thus, within the scope of this use case the cybersecurity non-experts that are trained on cutting edge technologies and the evolving 5G cybersecurity landscape.

5.2.3 PUC3: Cybersecurity Investment Decision Support

The goal of this use case is to **validate the capabilities of the SPIDER modelling and emulation platform to forecast and estimate the impact of cyber-risks**. In achieving this goal, SPIDER develops a decision support process via a software tool (entitled Cybersecurity Investment Component - CIC) that is integrated within the SPIDER Cyber Range as a Service (CRaaS) platform and does exactly that; given a certain 5G deployment, it identifies a best-fit suitable defensive strategy (i.e. a best-fit selection of mitigation controls that should be applied at the asset level so as to mitigate cyber-threats or vulnerabilities) subject to resource (e.g. financial budget) constraints. In doing so, CIC can support the relevant stakeholders to not only determine optimal investments to cybersecurity controls, but also to take the necessary steps to implement these controls towards minimizing the cyber-risks of a 5G infrastructure provider in a cost-effective way. The **CIC component** uses meaningful inputs to optimise the selection of the various actions related to the underlined cyber security resource allocation problem including the list of relevant assets existing in the 5G infrastructure, their relation and economic value, the identified vulnerabilities of the 5G infrastructure, the cyber risk exposure of the 5G infrastructure measured in economic terms, a set of controls that can be used to mitigate the vulnerabilities as well as budget constraints, rules, and additional preferences of the end user.

That's only a summary on **SPIDER's efficacy in supporting cybersecurity investment decisions** that are validated by demonstrating how the SPIDER's optimal investment strategy outperforms traditional investment and capital budgeting techniques. This is done by gauging the extent to which cyber-risk is hedged, when allowing for managerial discretion and combining real-time data on various cyber-risk metrics obtained from Continuous Risk Analysis Engine (CRAE) with economic uncertainty.

5.3 EVALUATION METHODOLOGY AND MEASURES SPECIFICATIONS

The evaluation methodology and measures specifications, as specified in D7.1 "Evaluation methodology and measures specifications" [6], has been developed within the SPIDER project with the main objective to provide an extended set of Key Performance Indicators (KPIs) and metrics for evaluation and analysis of the SPIDER pilot use cases and corresponding scenarios and user stories. Targeting a holistic evaluation process, the specified KPIs aims to guide the technical performance evaluation of the SPIDER platform, along with appropriate metrics to support evaluation on the front of user acceptance and user upskilling.

To this end, the specification initially provides the KPI and metric definition frameworks, identifying key aspects of the selected KPIs and metrics. Special attention is put to the technical performance evaluation, with respect to exploiting vulnerabilities related to 5G implementations, simulation and emulation scenarios and risk analysis, along with the impact of the proposed solution on the user perceived performance. At the same time, the specification includes the framework for the User Acceptance evaluation activities, defining the relative metrics. Fine grained KPIs are selected to support a closer look on the results and therefore enable the identification of potential limitations of the technological solutions presented by SPIDER.

The specific results derived from the evaluation plans, with relative stakeholders as participants, will be presented in the final reports of the project. SPIDER has described pilot validation procedure which consists of two iterations (i.e., M28-M32 and M33-M36). During these periods, the users/evaluators of the platform will interact with the different modalities and validate the platforms performance and usability according to the KPIs and metrics defined in this deliverable.

5.3.1 Metrics and KPIs Framework

The KPIs aim to capture important performance aspects reflecting on the quality of the service perceived by the end user and are selected based on the high-level project objectives, the cyber range's goals as well as, their applicability to the different pilot use cases. Furthermore, the identified KPIs aim to be Specific, Measurable, Attainable, Relevant, Timed (SMART), and simple to understand:

- Specific: Target a specific domain or field.
- Measurable: Quantifiable evaluation.
- Attainable: Achievable with the resources, technology, and the time available.
- Relevant: Evaluation and success relevant.

- Timed: Values can be collected within time-frames well-aligned with the project course e.g., facility readiness

The KPI framework followed by SPIDER has been derived to provide an enhanced evaluation framework aiming to cover both the SPIDER-developed components as well as, each individual scenario's requirements. It consists of 5 subcategories of Technical KPI's, those are: i) General, ii) 5G-focused, iii) Cybersecurity, iv) Machine Learning, v) Risk. The i) General category covers aspects that relate to the technical evaluation of the platform as a whole, ii) the 5G related KPI's are focused on the 5G aspects of the SPIDER platform, specifically related to MATILDA testbed, the iii) Cybersecurity subcategory analyses the KPI's that are related to the security components of the Security Assurance Platform as well as the needs of the scenarios for the cybersecurity testing and training. The iv) Machine Learning sets the KPI's for the SPIDER developed ML models and the v) Risk delves into the risk and investment support related KPI's.

5.3.2 Perceived Quality of Experience Metrics Framework

To the best of project's knowledge, the research on Perceptual quality metrics and User Acceptance metrics for cyber ranges is in its infancy. Therefore, at the time of writing this report, i.e. M30 (Dec '21), the project is developing a hybrid Quality of Experience (QoE) assessment framework based on relative research on adjacent technological markets (i.e., user acceptance and QoE evaluation of computer systems, software and telecommunication networks). The objective of the User Acceptance metrics is to determine the acceptability of different kinds of services (in this case we are focusing on a cyber range platform service). Using the work on user acceptance of computer technology[1], the project describes acceptability as the "prospective judgement" made by a group of potential users regarding the adoption of a given service or technology, whereas acceptance, refers to the actual adoption behaviour demonstrated by them when the service or technology is available. The assessment will build on the user-acceptance models proposed by Venkatesh and colleague[2] that correlate acceptance with the constructs of perceived usefulness and perceived ease-of-use.

The complete set of questions addressing all metrics will be contained in a questionnaire provided to end-users, adhering to the common, unified measurement methodology presented in the evaluation methodology and measures specifications framework. Questionnaires will be typically answered after the scenarios and games. When possible, objectively measured KPIs addressing the system's usability will serve as a complement to the self-assessed results.

[1] Davis, Fred D., Richard P. Bagozzi, and Paul R. Warshaw. "User acceptance of computer technology: A comparison of two theoretical models." Management science 35, no. 8 (1989): 982-1003.

[2] Venkatesh, Viswanath; Bala, Hillol (2008): Technology Acceptance Model 3 and a Research Agenda on Interventions. In Decision Sciences 39 (2), pp. 273–315.

5.4 SOCIAL IMPLICATIONS

The SPIDER project has been designed to have a positive societal impact by providing enhanced tools and technologies as well as an integrated Cyber Range as a Service solution to assist the next generation of telecommunication organisations to better prepare against complex cyber-attacks, ensuring as such a more cyber secure environment for all EU citizens. Next, we outline the positive societal impacts that are foreseen within SPIDER:

- An EU telecommunications industry better prepared for addressing threats to society originating from complex cyber-attacks targeting critical virtualised (5G) infrastructures,
- Improved security, resilience, and sustainability of telecommunications organisations (including TSPs, ISPs, TIPs, cloud providers, OTT players, etc.) against emerging cyber-threats,
- Reduced time and cost in 5G infrastructure operators, 5G network operators as well as cloud computing and mobile network technology providers for implementing cybersecurity solutions and for training their users to detect, block and mitigate cyber-attacks,
- Improved cybersecurity preparedness of 5G professionals (from staff in security operation centres to pen testers and risk managers) through improved cyber defence training,
- Improved understanding of the costs and investment decisions that need to be taken by 5G organisations towards securing their operations against cyber-attacks,
- Reduced societal fear of large-scale public safety disasters caused by cyber-attacks in the EU telecommunications sector,
- Increased social trust in the next generation telecommunications networks and systems.

Ultimately, SPIDER will contribute towards enhanced economic performance through encouraging further development and path to market for integrated cyber range solutions. The enhanced economic situation will also have a catalysing social impact through improved incomes and enhanced societal conditions within a wider societal context. In general, effective preparedness against emerging cyber threats is a business enabler, as it creates a safe environment for business development with reduced fear of theft of intellectual property or downtime due to cyber-attacks and contributes to increased flexibility in adopting new digital technologies in a safer manner.

In addition, the SPIDER consortium ensures the compliance of the performed activities with the basic ethical principles that represent the shared values upon which the European Union is founded and that are laid down in the European Charter of Fundamental Rights[3]. Due to the specificities of the targeted technological area, particular attention is placed on the potential impact of the project on privacy and data protection, including all GDPR elements, although it is not anticipated that there are any risks in this respect as no personal or sensitive data are involved. Existing training data sets are utilised by the project and not real-time telecommunications data, thus ensuring research integrity. Overall, the operational aspects of SPIDER are designed with privacy and data protection safeguards and are in accordance with GDPR's "*data minimisation*" principle.

Summing up, the text put together in this deliverable is fully aligned with the report given at the time of the proposal submission. No major societal issues have arisen during the execution of the project, besides of course the COVID-19 pandemic. The pandemic has demonstrated the critical importance that telecommunications infrastructures play in keeping businesses, governments, and societies connected and running. At the same time, the COVID-19 outbreak resulted to a significant upsurge in the total number of cyber-attacks targeting telecommunication organisations and individuals. In this

[3] EU Chapter of Fundamental Rights. Available online: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

respect, the SPIDER proposition seems to be aligned even to this new global prospect induced by the pandemic.

6 GENDER ISSUES

Over the years, the European Parliament has supported and called for measures to improve the position of women. This work continues through the activities of the Women's Committee. In this respect, several specific European and UN Policies have been adopted to promote the gender equity:

- Council Directive 75/117/EEC of 10 February 1975
- Council Directive 76/207/EEC of 9 February 1976
- Council Resolution of 29 May 1990
- Council Resolution of 27 March 1995
- Council Regulation (EC) No 2836/98 of 22.12.1998
- Council Directives 86/378/EEC of 24 July 1986 & 96/97/EC of 20 December 1996.

In carrying out the project activities, the SPIDER consortium promotes gender equality by fully respecting the above-mentioned policies. The project is committed to the strategy of the European Commission for equal promotion of women and men[4]. While it addresses the cybersecurity sector where the low percentage of women (7% of cybersecurity workforce, 11% globally) in leading positions has been identified as problematic in both academia and industry[5], the consortium pledges to follow the European strategy for gender equality for getting more women into the labour market and into high decision-making positions. Towards that, the consortium will include women as technology end-users in leading positions in the demonstrators, as scientists involved in leading research and as prominent speakers actively involved in technology demonstration.

Regarding the SPIDER impact, both women and men benefit equally from the project outcomes. Equal employment opportunities and equal treatment between men and women is guaranteed by taking actions covering: (1) the application of the principle of equal pay; (2) the creation of equal conditions for men and women with respect to access to employment, vocational training and retirement; (3) the equal treatment of the sexes in the area of the "de-jure" or "de-facto" social security systems; (4) the reversal of the burden of proof in cases of discrimination; and (5) the positive discrimination to promote the under-represented sex.

Overall, SPIDER has a strong female representation both in the technical team and among the executive members. The gender level of participation within the SPIDER project activities is being monitored throughout the project. At the time of writing this deliverable, i.e. M30 (Dec '21), the project core team has 25 women members taking a leading role and occupying different tasks, from exercise management and quality control (i.e., Dr. Irene Karapistoli, CLS) to work focused on concept design (i.e., Mr. Cristina Costa, FBK), software design (i.e., Mr. Chiara Lombardo, CNIT, and Mr. Carla Marcenaro, Ericsson) and systems' evaluation (i.e., Mr. Anna Angelogianni, UPRC). During SPIDER's pilots, we are also aiming at recruiting an equal number of men and women as test users. As acknowledged in SyGMA, and in the official Review Report, the SPIDER project demonstrated reasonable gender representation at all levels of personnel assigned to the action.

[4] Gender equality in Horizon Europe. Accessed online: https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/democracy-and-rights/gender-equality-research-and-innovation_en

[5] Center for Cyber Safety & Education, 2017 Global Information Security Workforce Study. https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

7 CONCLUSIONS

This deliverable has been produced with the aim to provide SPIDER's positioning concerning awareness and wider societal implications. Through its content a comprehensive analysis has been conducted to represent SPIDER project outcomes and organization from the perspective of practical as well as socially impacting issues and to highlight how gender issues are addressed by the project.

A summary of the values and benefits coming from the SPIDER solution provides an indication on how the project results have a clear and positive impact on various areas on the envisaged target markets also including the innovations around cybersecurity, and in particular, the cyber training capabilities identified within SPIDER.

The overview of the concrete set of activities that took place until the time of writing this deliverable, i.e. M30 (Dec '21), in the area of dissemination, exploitation and standardization has been thoroughly enlisted with the purpose of presenting the solid awareness framework that has been adopted and developed during the SPIDER project lifetime.

The analysis of the implications from a practical point of view is supported by elaborating from a technical perspective which are the SPIDER platform learning modalities along with a description of the demonstration strategy based on validation use cases and related methodology.

In addition, the societal implications considered in this deliverable clarifies how SPIDER solution aims to assist the next generation of telecommunication organisations ensuring a more cyber secure environment for all EU citizens.

Finally, the prospect on the gender issue provides indications of measures within the SPIDER consortium on how gender equality is promoted by fully respecting the European and UN Policies.

REFERENCES

[1] Grant Agreement Amendment AMD-833685-8 — SPIDER

[2] D2.5 “SPIDER user requirements and the 5G cybersecurity threat landscape – final version”

[3] D2.8 “SPIDER use cases and pilots definition – final version”

[4] D5.2 “SPIDER assurance and certification monitoring solutions”

[5] D6.2 “First integrated SPIDER platform prototype”

[6] D7.1 “Evaluation methodology and measures specifications”

[7] D8.1 “Plans for dissemination, communication, standardization and exploitation”

[8] D8.2 “Initial report on dissemination, communication, standardization and exploitation”

[9] D8.3 “Interim Report on dissemination, communication, standardisation, and exploitation”

[10] D8.6 “Report on connections with stakeholders and European CERTs/CSIRTs - initial version”