

DIGITAL EUROPE PROGRAMME (DIGITAL)

DIGITAL-ECCC-2022-CYBER-03-SEC-5G-

INFRASTRUCTURE



Security Assessments for Networks and services in 5G

D5.2 – Interim report on Dissemination, Exploitation, Standardisation & Sustainability

Abstract: This document will provide a description of all the activities for dissemination, collaboration, communication until the midterm of the project. It will also report on exploitation activities and roadmap for potential commercialization of the solution, as well as any standardization activities in the area. It will reflect outcomes from all Tasks in WP5.

Contractual Date of Delivery	30/06/2025
Actual Date of Delivery	30/06/2025
Deliverable Security Class	Public
Editor	OQTECH
Contributors	UPAT, SPH, p-NET, WINGS, OQTECH, NCSA, ADAE
Quality Assurance	SPH, NCSA



This deliverable describes work undertaken in the context of the SAND5G project, “Security Assessments for Networks and Services in 5G” which has received funding from the European Union’s Digital Europe programme under grant agreement No 101127979 and is supported by European Cybersecurity Competence Center. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Document Revisions & Quality Assurance

Internal Reviewers

SPH, NCSA

Revisions

Version	Date	By	Overview
0.0	14/02/2025	OQTECH	Table of Contents and First draft contents
0.1	07/05/2025	OQTECH	Contributions from UPAT, PNET, OQTECH
0.2	18/05/2025	OQTECH	List of tables, list of figures
0.3	21/05/2025	OQTECH	Final contributions for chapter 4 & 5 and full draft for internal review
0.4	26/05/2025	OQTECH	Document sent for internal review.
0.5	03/06/2025	NCSA	Review #1 completed
0.6	04/06/2025	SPH	Review #2 completed
0.7	13/06/2025	OQTECH	Comments of the reviews are addressed and creation of 2nd draft
1.0	27/06/2025	UPAT	Final version to be submitted

Contents

List of Figures	4
List of Tables.....	5
List of Abbreviations	1
1 Introduction	3
2 Dissemination & Communication	4
2.1 Dissemination Activities	4
2.1.1 Journal and Conference Publications	4
2.1.2 Webinars – Workshops.....	7
2.1.3 Events – Exhibitions.....	11
2.2 Communication Activities.....	23
2.2.1 Website.....	23
2.2.2 Social Media	24
2.2.3 Newsletters.....	26
2.2.4 Press Releases.....	29
2.2.5 Promotional Material	29
2.2.6 Updated Communication Plans	32
2.3 Engagement Approaches and Channels with stakeholders	33
3 Exploitation & Sustainability Activities	35
3.1 Partners’ Individual Exploitation Plans.....	35
3.2 SAND5G Exploitation Process.....	42
3.2.1 Characterization of Project Results	42
3.2.2 Identification of Key Exploitable Results (KERs)	43
3.2.3 Go-to-Market Roadmap	43
4 Clustering and Standardization.....	46
4.1 Clustering Activities and Plans.....	46
4.1.1 Clustering Objectives.....	46
4.1.2 Project Landscape Mapping	47
4.1.3 EU-Funded Projects	47
4.1.4 Clustering Activities & Methodology.....	53
4.2 Standardization Activities and Plans	53
4.2.1 Goals for standardization and a strategic framework	53
4.2.2 Target Standardization Bodies and Engagement Strategy	54
5 Conclusions	56

List of Figures

Figure 1. Special Issue: Cybersecurity in the 5G Era - Official Call	5
Figure 2. Special Issue: Cybersecurity in the 5G Era - Keywords	5
Figure 3. Special Issue: Recent Applications of Field-Programmable Gate Arrays (FPGAs) - Official Call	6
Figure 4. Special Issue: Recent Applications of Field-Programmable Gate Arrays (FPGAs) - Keywords. 6	
Figure 5. 1 st Webinar: Through the Lens of SAND5G - Invitation to register	7
Figure 6. Statistics of registered participants and attendance at 1st Webinar	8
Figure 7. Presenters of the 1st Webinar “5G Networks Security through the lens of SAND5G”	8
Figure 8. Save the date poster for the 2nd Webinar “Cross-border Cybersecurity through the Lens of Government”	9
Figure 9. p-NET’s booth at TEDxPatras 2025, and SAND5G flyers distributed.	10
Figure 10. Workshop held, with the banner displayed at the venue.	11
Figure 11. SAND5G at DSD 2024	12
Figure 12. SAND5G at IEEE 2024	13
Figure 13. SAND5G 1st Plenary meeting in Patras.....	14
Figure 14. SAND5G in Advanced Telecoms & IoT summit 2024	15
Figure 15. SAND5G in Edge Computing at ETCEI 2024	16
Figure 16. SAND5G at InfoCom World 2024	17
Figure 17. SAND5G 3rd Plenary Meeting in Athens.....	18
Figure 18. SAND5G at CYSAT 2025 in Paris	19
Figure 19. SAND5G in IOSEC 2025	20
Figure 20. SAND5G in MECO 2025	21
Figure 21. SAND5G 4th Plenary and training meeting.....	22
Figure 22. SAND5G website traffic and visitors metrics	24
Figure 23. SAND5G Linkedin metrics for the past year	25
Figure 24. SAND5G 1st Newsletter cover	26
Figure 25. SAND5G 2nd Newsletter cover	27
Figure 26. SAND5G 3rd Newsletter cover.....	28
Figure 27. SAND5G brochure	30
Figure 28. SAND5G brochure	30
Figure 29. SAND5G pull up banner	31
Figure 30. Triangle of Actors collaboration Model	33
Figure 31. SAND5G Stakeholder Matrix.....	33
Figure 32. SAND5G Stakeholder engagement process	34
Figure 33. Value Proposition Canvas	44

List of Tables

Table 1. UPAT Exploitation Plan.....	35
Table 2. SPH Exploitation Plan	36
Table 3. p-NET Exploitation Plan.....	37
Table 4. WINGS Exploitation Plan	38
Table 5. OQ Technology Exploitation Plan.....	39
Table 6. ADAE Exploitation Plan.....	40
Table 7. NCSA Exploitation Plan.....	41
Table 8. Template of Characterization Table.....	43
Table 9. SAND5G partners' participation in other EU projects.....	52

List of Abbreviations

3GPP	3rd Generation Partnership Project
5G	(Mobile) Fifth Generation
6G-IA	6G Smart Networks and Services Industry Association
CACAO	Collaborative Automated Course of Action Operations
CRIRM	Cyber Range, Insurance, and Risk Management
CSR	Cyber Security and Resilience
CYSAT	Cybersecurity for the Space Industry
dKPI	Dissemination Key Performance Indicator
DSD	Digital System Design
ENISA	European Union Agency for Cybersecurity
ETCEI	Emerging Tech Conference: Edge Intelligence
ETSI	European Telecommunications Standards Institute
FPGA	Field-Programmable Gate Array
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IM	Innovation Manager
IMC	Innovation Management Committee
IOSEC	Information and Operational Technology Security
ISO	International Organization for Standardization
ISSN	International Standard Serial Number
KER	Key Exploitable Result
KPI	Key Performance Indicator
MDPI	Multidisciplinary Digital Publishing Institute
MECO	Mediterranean Conference on Embedded Computing
PoC	Proof of Concept
R&I	Research & Innovation
SAND5G	Security Assessments for Networks and Services in 5G

UVP	Unique Value Proposition
WP	Work Package

1 Introduction

This document is an interim report on the dissemination and communication activities that the SAND5G project has undertaken during the first 18 months of its life. As described in the previous deliverable for Work Package 5 (D5.1 – Plan on Dissemination, Exploitation, Standardisation & Sustainability), the project aimed to make use of activities such as publications in journals, books and conferences, white papers, demonstrations, presentations at various relevant events, etc.

The structure of this document gives a detailed account of all the aforementioned activities, starting with the **Dissemination and Communication** activities in **Section 2**, continuing with the **Exploitation and Sustainability** activities in **Section 3** and finishing with **Clustering and Standardization** activities in **Section 4**.

The authors of this deliverable tried to include all of the information on the dissemination and communication activities the project as a whole, but also the individual partners, were involved, including presentation of SAND5G during public events, press releases, newsletters, webinars, social media, promotional materials, etc.

2 Dissemination & Communication

2.1 Dissemination Activities

2.1.1 Journal and Conference Publications

UPAT has actively contributed to the dissemination of the SAND5G project through a set of peer-reviewed scientific publications in high-profile conferences and journals. Below is a categorized overview of the contributions so far.

Journal Papers (Submitted or In Progress):

- Dionysia Varvarigou, Kostas Lampropoulos, Christos Tranoris, Aimilia Bantouna, Karim Baccar, Andreas Stamoulis, Kostas Poulis, Lampros Raptis, Paris Kitsos. *"SAND5G – Strengthening 5G with Security Assessments for Networks and Services"*, submitted to **Elsevier – Microprocessors and Microsystems** (under review).

Conference Papers (Published or Accepted):

- Marios Papadopoulos, Konstantinos Lampropoulos and Paris Kitsos, «An FPGA Architecture of Authentication and Key Agreement (AKA) Protocol for 5G Networks», accepted for presentation at the 28th Euromicro Conference Series on Digital System Design (DSD 2025) in Salerno, Italy, September 2025.
- Dionysia Varvarigou, Kostas Lampropoulos, Odysseas Koufopavlou, Spyros Denazis, Paris Kitsos. "An Efficient Methodology for Real-Time Risk and Impact Assessment in 5G Networks". 2025 IEEE International Conference on Cyber Security and Resilience, Crete, Greece, August 2025.
- Marios Papadopoulos, Kostas Lampropoulos, Paris Kitsos, "An FPGA Architecture of Extensible Authentication Protocol EAP- AKA' for 5G Networks", 14th Mediterranean Conference on Embedded Computing (MECO 2025), Budva, Montenegro, 10-14, June 2025.
- Kostas Lampropoulos, Kostas Pournaras, Christos Tranoris, Odysseas Koufopavlou, Spyros Denazis, Paris Kitsos. "SAND5G – Security Assessments for Networks and Services in 5G Networks: From 5G to Edge", presented at the 3rd Emerging Tech Conference: Edge Intelligence (ETCEI 2024) in Volos, Greece.
- Marios Papadopoulos, Kostas Lampropoulos, Paris Kitsos. "FPGA-Based Cloud Security Solutions for 5G Networks", presented at the IEEE International Conference on Cyber Security and Resilience (CSR 2024) in London, UK.
- Aimilia Bantouna, Paris Kitsos, Kostas Lampropoulos, Kostas Poulis, Omar Qaise, Lampros Raptis, Andreas Stamoulis and Christos Tranoris. "Security Assessments for Networks and Services in 5G Networks", presented at the 27th Euromicro Conference Series on Digital System Design (DSD 2024) in Paris, France.

Special Issue Contributions (In Preparation):

Two special issue submissions are currently being prepared. Screenshots with the guest editors and relevant keywords are included below for reference.

- *"Intrusion Detection and Resilience in 5G: Towards Automated Threat Response"*, for the **Special Issue: Cybersecurity in the 5G Era, Network (ISSN: 2673-9517)**, MDPI. The following two figures present the official call for papers of this special issue, with its keywords.

Special Issue Editors



Dr. Kostas Lampropoulos [E-Mail](#) [Website](#)

Guest Editor

Electrical and Computer Engineering Department, University of Patras, 26500 Patras, Greece

Interests: identity management; privacy; cybersecurity; network security



Dr. Alexios Lekidis [E-Mail](#) [Website](#)

Guest Editor

Department of Energy Systems, University of Thessaly, Gaiopolis Campus, 41500 Larissa, Greece

Interests: Industrial Internet of Things; network-based intrusion detection; incident response; 5G and next-generation networks; intelligent energy systems; vehicle-to-everything

Special Issues, Collections and Topics in MDPI journals



Prof. Dr. Paris Kitsos [E-Mail](#) [Website1](#) [Website2](#)

Guest Editor

1. Electrical and Computer Engineering Department, University of Patras, 26504 Patras, Greece

2. Electrical and Computers Engineering Department, University of the Peloponnese, 22131 Patras, Greece

Interests: efficient implementations of cryptographic; 5G security; IoT security; DSP and ML primitives

Special Issues, Collections and Topics in MDPI journals

Figure 1. Special Issue: Cybersecurity in the 5G Era - Official Call

Keywords

- 5G networks
- cybersecurity
- privacy
- resilience
- intrusion detection
- access control

Figure 2. Special Issue: Cybersecurity in the 5G Era - Keywords

- "Security-Oriented FPGA Architectures for 5G Systems", for the **Special Issue: Recent Applications of Field-Programmable Gate Arrays (FPGAs), Applied Sciences (ISSN: 2076-3417)**, MDPI. The following two figures present the official call for papers of this special issue, with its keywords.

Special Issue Editors



Dr. Mirosław Chmiel E-Mail Website

Guest Editor

Department of Digital Systems, Silesian University of Technology, Konarskiego 18a St., 44-100 Gliwice, Poland

Interests: digital systems; control systems; reconfigurable control systems; embedded systems; systems-on-a-chip, programmable logic controllers; Industry 4.0



Prof. Dr. Paris Kitsos E-Mail Website1 Website2

Guest Editor

1. Electrical and Computer Engineering Department, University of Patras, 26504 Patras, Greece

2. Electrical and Computers Engineering Department, University of the Peloponnese, 22131 Patras, Greece

Interests: efficient implementations of cryptographic; 5G security; IoT security; DSP and ML primitives

Special Issues, Collections and Topics in MDPI journals

Figure 3. Special Issue: Recent Applications of Field-Programmable Gate Arrays (FPGAs) - Official Call

- Synthesis and implementation methods exploiting device-specific architecture elements, hard macros, and IP cores.
- Design methodologies.
- Verification and validation techniques, including formal verification methods.
- Optimization techniques (e.g., power, area, delay).
- Performance evaluation.
- The implementation of intelligent algorithms directly in hardware.
- AI/ML on FPGAs.
- Hardware architectures for 5G/6G networks.
- Reconfigurable architectures, including reconfigurable control systems.
- Dependable systems (cryptology, security algorithms, security aspects).
- Non-trivial applications, including the following:
 - Real-time systems, real-time sensing, and computing.
 - Systems-on-a-chip (SoC).
 - Industrial control: programmable logic controllers, dedicated CPUs, flexible and expandable I/O modules, dedicated network controllers.
 - Digital signal processing.
 - Internet of things.

Figure 4. Special Issue: Recent Applications of Field-Programmable Gate Arrays (FPGAs) - Keywords

KPI Satisfaction:

- dKPI-1.6.1 (>6 publications in international referred journals and conferences): 6 conference publications + 1 journal submission = 7 total (100%)
- dKPI-1.6.2 (>2 journal special issues): 2 journal special issues being prepared (67%)
- dKPI-1.6.4 (>12 conference presentations): 4 accepted conference presentations + 1 under review + 2 accepted for 2025 = 7/12 (55%)
- dKPI-3.1.1 (Participation in >10 small and large-scale events by the end of the project): 4 major events participated in (40%) only from publications

2.1.2 Webinars – Workshops

As part of its communication and engagement activities, p-NET Emerging Networks & Applications, a partner of SAND5G, is organizing a series of webinars titled **"Through the Lens of..."**. Each webinar will explore key cybersecurity topics - each examined from a unique perspective.

The first webinar in the series, **"5G Networks Security Through the Lens of SAND5G,"** marked the official launch of this initiative. Held on April 30, 2025, the session aimed to present core elements of the project's approach to enhancing 5G security, while fostering engagement with stakeholders from industry, government, and academia.

Held online, the webinar featured expert discussions on the evolving risks associated with 5G networks and the corresponding EU policy and regulatory frameworks. Presentations also included a demonstration of the SAND5G risk and impact assessment platform, showcasing the use of machine learning for real-time threat detection and automated response capabilities.

The webinar emphasized the importance of cross-sector collaboration and the role of innovative tools in securing 5G infrastructures. It contributed to raising awareness of the project's objectives and fostered dialogue on best practices and future directions for 5G cybersecurity in the EU.



Figure 5. 1st Webinar: Through the Lens of SAND5G - Invitation to register

As noted below, the number of participants who registered for the event amounted to 67 while 63 participants attended the webinar.

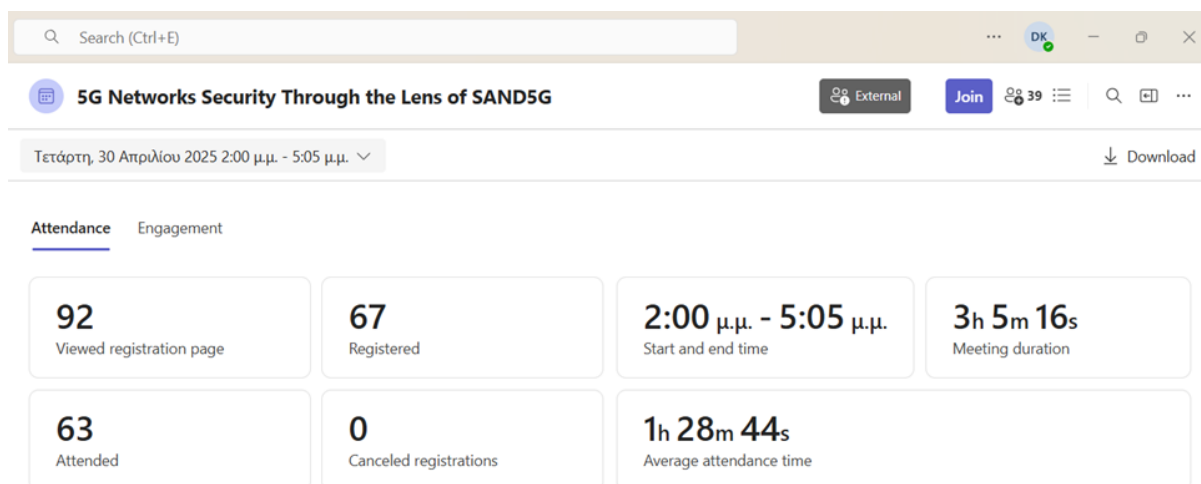


Figure 6. Statistics of registered participants and attendance at 1st Webinar



Figure 7. Presenters of the 1st Webinar “5G Networks Security through the lens of SAND5G”

The Workshop was organized as part of SAND5G’s broader strategy to support capacity building and stakeholder engagement, in alignment with EU cybersecurity priorities. More information is available at: [Implemented Training Events - Sand5G](#)

On July 2nd, 2025, the second webinar of the “Cybersecurity: Through the Lens of...” series is scheduled to take place. Under the title “**Cross-border Cybersecurity through the Lens of Government**” it will host high-level experts representing national governments and leading cybersecurity agencies.

The speakers will share how public sector leaders are addressing cross-border cybersecurity threats and enhancing collaboration in an increasingly interconnected digital landscape.



Figure 8. Save the date poster for the 2nd Webinar “Cross-border Cybersecurity through the Lens of Government”

Future webinars in the series will continue to explore cybersecurity topics from the perspectives of national authorities, industry, and the research and innovation community.

On May 17, 2025, the SAND5G project supported the organization of an interactive **cybersecurity workshop** titled “**Think Before You Click! To Hackers, the Easiest Target is You!**”, held at the University of Patras Conference Center during TEDxPatras 2025.

The session, led by cybersecurity researchers from the University of Patras, focused on raising awareness of everyday digital risks and promoting safe online behaviors. Through real-life scenarios and practical advice, participants were engaged in discussions around personal cybersecurity and digital resilience.

In addition to the workshop, an interactive booth organized by p-NET Emerging Networks & Applications provided participants with insights into EU cybersecurity, including flyers of the SAND5G project.

The event was held in collaboration with other EU-funded initiatives, the CURIUM and CUSTODES projects, reflecting the strong synergy among European efforts to promote cybersecurity awareness and competence. This workshop was part of SAND5G's broader mission to engage the public and strengthen cybersecurity capacity across diverse audiences.

The number of participants who attended the Workshop amounted to 45, whereas the number of SAND5G flyers distributed at p-NET's booth was 30.



Figure 9. p-NET's booth at TEDxPatras 2025, and SAND5G flyers distributed.



Figure 10. Workshop held, with the banner displayed at the venue.

2.1.3 Events – Exhibitions

Partners that are participating in the SAND5G project attended a number of events, conferences and summits that allowed the promotion of the project. During these events, we tried to show visibility through visual materials, such as pop-up banners or presentations and engage with other participants in order to inform them on all aspects of the project.

UPAT - UPAT has actively participated in several high-visibility events and exhibitions to promote the SAND5G project to both the scientific community and industry stakeholders. UPAT represented the project at the 3rd Emerging Tech Conference: Edge Intelligence (ETCEI 2024) in Volos, Greece, presenting the paper “SAND5G – Security Assessments for Networks and Services in 5G Networks: From 5G to Edge”, which attracted interest from both academic and industry participants working on edge intelligence and 5G infrastructure. Additionally, UPAT contributed to the IEEE International Conference on Cyber Security and Resilience (CSR 2024) in London, UK, through the presentation “FPGA-Based Cloud Security Solutions for 5G Networks”, strengthening visibility among cybersecurity experts and practitioners.

Moreover, UPAT showcased SAND5G research outcomes at the 27th Euromicro Conference on Digital System Design (DSD 2024) in Paris, France. This venue served as a platform to engage with researchers and industrial representatives in embedded and secure system design. These participations significantly supported the dissemination strategy and contributed to KPIs regarding conference attendance and outreach to targeted stakeholders.

UPAT also supported the design and dissemination of promotional material (e.g., banners and leaflets) during these events, ensuring a consistent and recognizable project identity. The team continues to explore additional opportunities to exhibit SAND5G results at upcoming regional and international cybersecurity and networking events during the next reporting period.

In addition to UPAT's direct contributions, the SAND5G project has participated in more than 10 high-visibility events and exhibitions across Europe. A full list of project-level participations is maintained and publicly accessible through the official project website's (<https://sand5g.eu>) News & Events section.

As a result, KPI dKPI-3.1.1 (Participation in >10 small and large-scale events) is already **fully satisfied**.

SAND5G @ DSD 2024

By SAND5G || Published On: 03/09/2024 || Categories: 5G, Networks, Security

It was a great pleasure to be part of the 50th anniversary of Euromicro in Paris, France. As part of the DSD 2024 conference, the SAND5G project was presented. During the networking sessions of the conference, very interesting speeches about the project and security in 5G took place with other researcher/professors. The proceedings of the conference will be available soon, so keep in touch.



Figure 11. SAND5G at DSD 2024

SAND5G participation at 2024 IEEE International Conference on Cyber Security and Resilience in London

By SAND5G || Published On: 19/09/2024 || Categories: 5G, Networks, Security



A very interesting research paper was presented at the 2024 IEEE International Conference on Cyber Security and Resilience, held from September 2 to 4, 2024, in London, titled "FPGA-based Cloud Security Solutions for 5G Networks." The event was a great opportunity for SAND5G to exchange ideas on the security of 5G. Through presentations and informal discussions, SAND5G's dissemination took place, and very interesting security extensions to cloud computing and IoT were introduced.

Figure 12. SAND5G at IEEE 2024

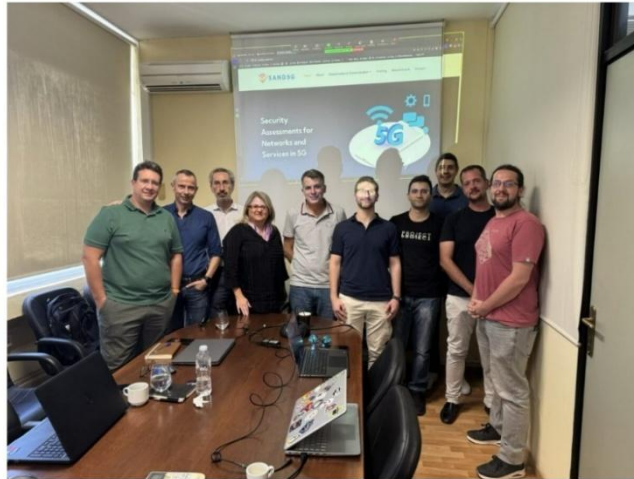
SAND5G 1st Plenary Meeting

By SAND5G || Published On: 09/10/2024 || Categories: 5G, Networks, Security

Representatives from all partner organizations in the SAND5G consortium convened in Patras on October 4th, 2024, for a highly productive plenary meeting.

Participants engaged in insightful discussions and presentations, with work package and task leaders outlining the advancements made during the project's first nine months.

The meeting concluded with a clear roadmap for the upcoming phase, as task and work package leaders defined their objectives, established timelines, and emphasized key actions for the future, ensuring SAND5G remains on track.



For more direct updates regarding SAND5G, follow us on [LinkedIn](#) and [X](#).

For regular updates, including a curated selection of news and pertinent information, please subscribe to our [Newsletter](#).

Figure 13. SAND5G 1st Plenary meeting in Patras

SAND5G Participation in Advanced Telecoms & IoT Summit 2024

By SAND5G || Published On: 14/10/2024 || Categories: 5G, Networks, Security

SAND5G was actively represented at the SPHYNX booth during the Advanced Telecoms & IoT Summit 2024, held on October 8, 2024, at Zappeion Megaro in Athens. The event aimed to promote innovative solutions, applications, and services that utilize advanced telecommunications infrastructures, such as 5G networks, fiber optic networks to the building (FTTH/B), wireless broadband networks (FWA), IoT, satellites, and more.

Prof. George Spanoudakis, CEO of Sphynx Technology Solutions, delivered a significant speech about the SAND5G project during the "Advanced Infrastructures: Upcoming Developments" session, attended by established partners and a high-level audience.

The event generated considerable interest, facilitating the exchange of ideas with high-value companies, focusing on equipping the 5G ecosystem with actionable insights and enhancing cybersecurity strategies and policies.



Figure 14. SAND5G in Advanced Telecoms & IoT summit 2024

SAND5G @ ETCEI 2024 Conference

By SAND5G || Published On: 22/10/2024 || Categories: 5G, Networks, Security

The 2024 edition of the **Emerging Tech Conference Edge Intelligence** (ETCEI) was held from 17 to 18 October in Volos, Greece. The ETCEI 2024, was organized by **Hellenic Emerging Technologies Industry Association** (HETIA) with the primary aim of highlighting the synergies and results of the cooperation between academic and research institutions and their researchers with entrepreneurial entities in cutting-edge technology fields.

Prof. Paris Kitsos, presented a poster (entitled "SAND5G – Security Assessments for Networks and Services in 5G Networks: From 5G to Edge" by Kostas Lampropoulos, Kostas Pournaras, Christos Tranoris, Odysseas Koufopavlou, Spyros Denazis, Paris Kitsos) which described and very important extension of the SAND5G security concept to Edge computing.

The event greatly enhanced SAND5G's visibility among businesses and academics, resulting in the establishment of several new business connections that could lead to future collaborations.

For more direct updates regarding our project, follow us on [LinkedIn](#), [X](#) and [Youtube](#).

For regular updates, including a curated selection of news and pertinent information, please subscribe to our [Newsletter](#).



Figure 15. SAND5G in Edge Computing at ETCEI 2024

SAND5G at InfoCom World 2024

By SAND5G || Published On: 25/11/2024 || Categories: 5G, Networks, Security

On November 12, 2024 SAND5G presented at [InfoCom World 2024](#). In more detail, Kostas Poullos from Sphynx participated in a Round Table discussion on the topic *"The Need for the Digital Transformation Leap"*, where they addressed very important Cybersecurity issues.

The InfoCom World 2024, titled this year as "Digital Greece: Time for a Leap!", took place on November 12, 2024, at the Divani Caravel Hotel in Athens. The annual meeting point for the Technology, IT, and Telecommunications market focused on the dynamic growth of the country through the adoption and utilization of new technologies, the challenges and opportunities arising, and the steps stakeholders in the market need to take to achieve the "digital leap"!



For more direct updates regarding our project, follow us on [LinkedIn](#), [X](#) and [Youtube](#).

For regular updates, including a curated selection of news and pertinent information, please subscribe to our [Newsletter](#).

Figure 16. SAND5G at InfoCom World 2024

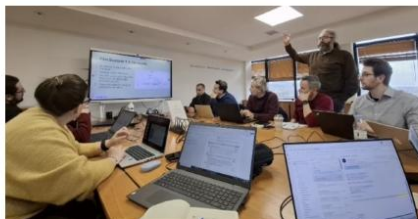
SAND5G 3rd Plenary Meeting

By SAND5G || Published On: 24/02/2025 || Categories: News

We are delighted to announce the successful conclusion of the 3rd plenary meeting, on the 21st of February 2025. The event hosted by [Sphynx](#) and [OQ Technology](#) at the offices of [5G Ventures S.A | Phaistos Investment Fund](#) in Athens.

The partners of SAND5G have discussed the project progress and outcomes so far and to plan our work for the second year of the project. The collaborative atmosphere and partners' dedication has been fundamental in the success of the plenary.

Thank you to all our partners for their active participation, invaluable insights, and continued dedication.



For more direct updates regarding our project, follow us on [LinkedIn](#), [X](#).

For regular updates, including a curated selection of news and pertinent information, please subscribe to our [Newsletter](#).

Figure 17. SAND5G 3rd Plenary Meeting in Athens

SAND5G will be presented at CYSAT 2025 in Paris

By SAND5G || Published On: 17/03/2025 || Categories: News

SAND5G will be presented on **CYSAT 2025** in Paris on 14–15 May 2025. **OQ Technology** which is a major pilot for the validation of the SAND5G platform will participate in the biggest CyberSecurity for the Space Industry event in Europe.

Through the presentations and networking sessions, SAND5G's dissemination will take place, and very interesting security extensions to space applications will be introduced.



For more direct updates regarding our project, follow us on [LinkedIn](#), [X](#).

For regular updates, including a curated selection of news and pertinent information, please subscribe to our [Newsletter](#).

Figure 18. SAND5G at CYSAT 2025 in Paris

SAND5G supports IOSEC 2025

By SAND5G || Published On: 29/04/2025 || Categories: News

Mark your calendars for **August 4–6, 2025**, for an immersive scientific workshop in **Chania, Crete, Greece**. **IOSEC 2025**, supported by **SAND5G** project, held alongside the IEEE CSR 2025 conference, promises insightful discussions on cutting-edge topics in cybersecurity.

Call for Papers: We invite authors to submit their original, unpublished work on a wide array of subjects. This is your chance to contribute to the advancement of information and operational technology security. **One week remains until final submission!**

Important Dates:

- Paper submission deadline: ~~April 14~~ **May 5, 2025** (extended, firm)
- Authors' notification: ~~May 5~~ **May 26, 2025**
- Camera-ready submission: ~~May 26~~ **June 16, 2025**
- Registration deadline (authors): ~~May 26~~ **June 16, 2025**
- Workshop dates: **August 4–6, 2025**

Learn More: <https://www.ieee-csr.org/iosec> for detailed information and submission guidelines.

Seize the opportunity to engage with leading experts, exchange ideas, and shape the future of cybersecurity. We look forward to your participation!

Figure 19. SAND5G in IOSEC 2025

SAND5G participation at 14th Mediterranean Conference on Embedded Computing (MECO 2025)

By SAND5G || Published On: 03/06/2025 || Categories: 5G, Networks



A very interesting research paper was accepted and it will be presented at the 14th Mediterranean Conference on Embedded Computing (MECO 2025) in Budva, Montenegro, titled "An FPGA Architecture of Extensible Authentication Protocol EAP-AKA' for 5G Networks" by Papadopoulos Marios, Konstantinos Lampropoulos and Paris Kitsos.

The event will be a great opportunity for SAND5G to exchange ideas on the security of 5G and future networks.

Figure 20. SAND5G in MECO 2025

SAND5G Plenary and Training Meeting

By SAND5G | Published On: 18/06/2025 | Categories: News, Training Activities

On June 12th, 2025, SAND5G held a productive and insightful training session at Patras Science Park, organized and hosted by p-NET. The internal training aimed to educate and prepare relevant SAND5G team members for the kick-start of the planned pilot activities. Focused trainings covered the specificities of all foreseen pilot cases.

Pilot trainings were given by:

- Dr. Dionysia Varyngou from the University of Patras;
- Sotiris Katsimbas from OCJ Technologies;
- Amilia Bantouna from WINGS.

Each session offered valuable insights into the pilot architecture, data integration strategies, technical requirements on the SAND5G platform, and use case scenarios.

This training session marked an important step in enhancing the technical expertise and operational readiness of the teams involved, helping to advance the development of SAND5G's innovative 5G-enabled solutions.



Next day, on June 13th, 2025, the SAND5G consortium held a very important Plenary Meeting, which was also organized and hosted by p-NET.

The meeting provided a crucial platform for partners to review progress, align on next steps, and discuss the latest advancements in the project's pilot implementations. The collaborative environment fostered strategic discussions that will drive the continued innovation and success of SAND5G's 5G-enabled solutions.



For more direct updates regarding our project, follow us on [LinkedIn](#), [X](#).

For regular updates, including a curated selection of news and pertinent information, please subscribe to our [newsletter](#).

Figure 21. SAND5G 4th Plenary and training meeting

2.2 Communication Activities

As the lead partner for communication activities in SAND5G, UPAT is responsible for the strategic design, coordination, and execution of the project's external communication plan. The primary goal is to ensure that key messages about the project's objectives, outcomes, and impacts reach a wide range of stakeholders, including academic communities, industry, policy makers, and the general public. Communication efforts focus on increasing awareness, visibility, and engagement with the SAND5G results by leveraging multiple channels, both digital and physical. These include the official project website, social media platforms, newsletters, press releases, and promotional materials, as well as updated communication planning aligned with the project's evolving roadmap.

This section outlines the main communication tools and activities implemented until the midterm of the project, organized under the following categories: website management (3.2.1), social media presence (3.2.2), newsletter publication (3.2.3), press releases (3.2.4), development of promotional material (3.2.5), and updates to the communication strategy (3.2.6). Each subsection provides a detailed overview of the efforts made, content created, and progress toward communication KPIs set in D5.1.

2.2.1 Website

The official SAND5G website (<https://sand5g.eu>) was launched early in the project and has been actively maintained by UPAT. It serves as a central hub for external communication and dissemination, offering timely updates on project objectives, milestones, events, publications, and public deliverables. The website is structured into several user-friendly sections, including *About*, *Dissemination & Communication* (covering Deliverables, Workshops & Demos, Publications, Brochures & Flyers, Press Releases, and Newsletters), *Training*, *News & Events*, and *Contact*.

During the first 18 months, the site has been regularly updated with new content reflecting project progress. Public deliverables such as D5.1, press releases, partner contributions, and announcements about conference participations have been uploaded. A blog-style *News* section has been added to provide visibility into key activities and upcoming engagements. Additionally, the newsletter subscription form is available online and monitored by the UPAT team.

In terms of performance, website analytics indicate an increasing trend in engagement, with average monthly visitors exceeding the KPI threshold of 20, and over 100 site access instances recorded during the first year. These figures are expected to grow as more technical outputs and pilot activities become publicly available.

The website also provides direct access to the project's social media accounts, enhancing cross-channel engagement. Overall, the site remains an essential pillar in SAND5G's communication strategy, supporting transparency, stakeholder engagement, and outreach across all target groups.

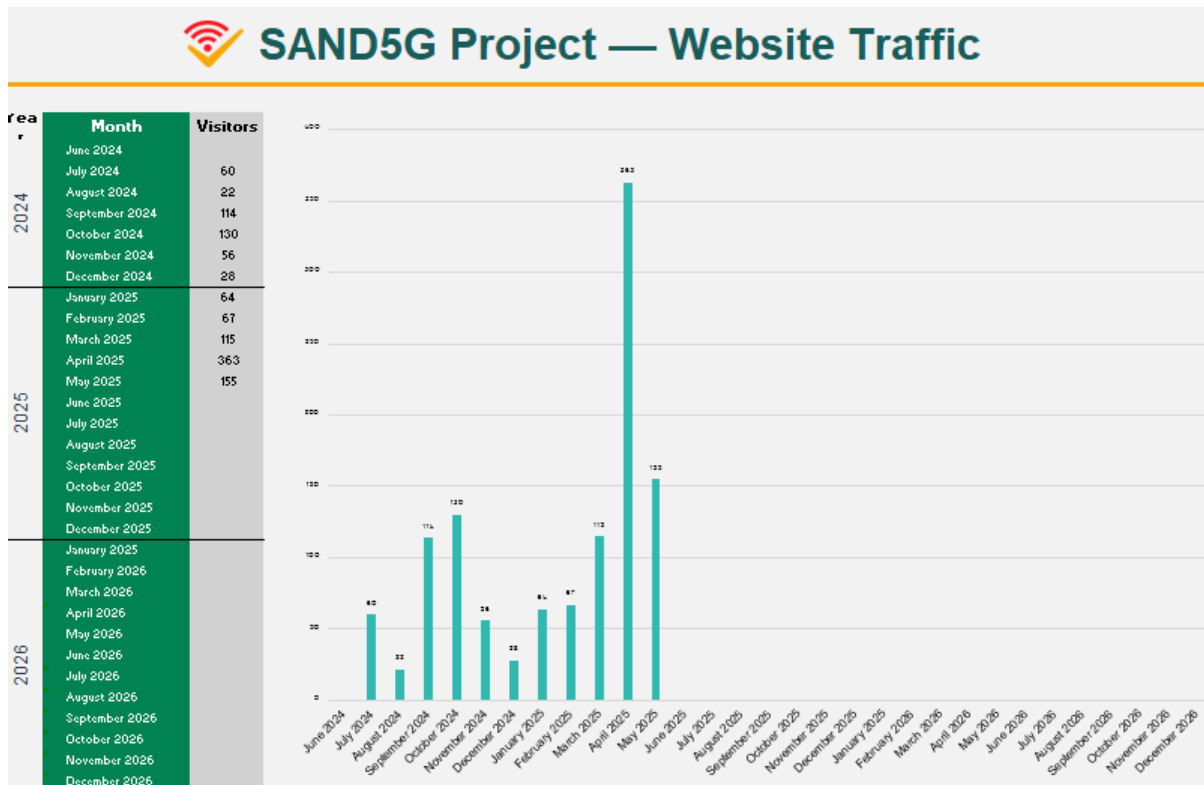


Figure 22. SAND5G website traffic and visitors metrics

KPI Satisfaction:

- dKPI-1.1.1 (>20 website visitors monthly): > 100 per month – **fully satisfied**
- dKPI-1.1.2 (>1000 site access times annually): >1100 - **fully satisfied**

2.2.2 Social Media

To maximize visibility and engage with diverse stakeholder groups, UPAT manages and coordinates the SAND5G social media presence across three platforms: **LinkedIn** ([@SAND5G EU Project](#)), **X (formerly Twitter)** ([SAND5G project](#)), and **YouTube** ([SAND5G Channel](#)). These platforms serve as key communication channels to disseminate news, share project milestones, announce publications and events, and promote partner activities.

Throughout the first 18 months of the project, UPAT has developed and implemented a consistent content strategy using dedicated hashtags such as **#SAND5G**, **#CyberSecurity**, and **#5GSecurity**. Regular posts have highlighted publications, conference participations, deliverable releases, and project-related news. Content has been designed with visual consistency, using banners, infographics, and animated elements aligned with the project's visual identity.

Performance metrics show strong engagement on LinkedIn, with over 22 new followers per month and more than 60 monthly profile views, exceeding the defined KPIs. X activity is also growing, with retweets and mentions from related EU-funded projects, increasing SAND5G's reach within the cybersecurity and 5G research communities. Although YouTube activity is currently limited, the platform is in place and will host video content (e.g., animated explainers and training material) in the upcoming period.

Social media accounts are also cross-linked with the website, enabling a seamless flow of information and enhancing discoverability. Overall, social media remains a vital tool in the communication ecosystem of SAND5G, helping build a community around the project and raising awareness among academic, industrial, and public stakeholders.

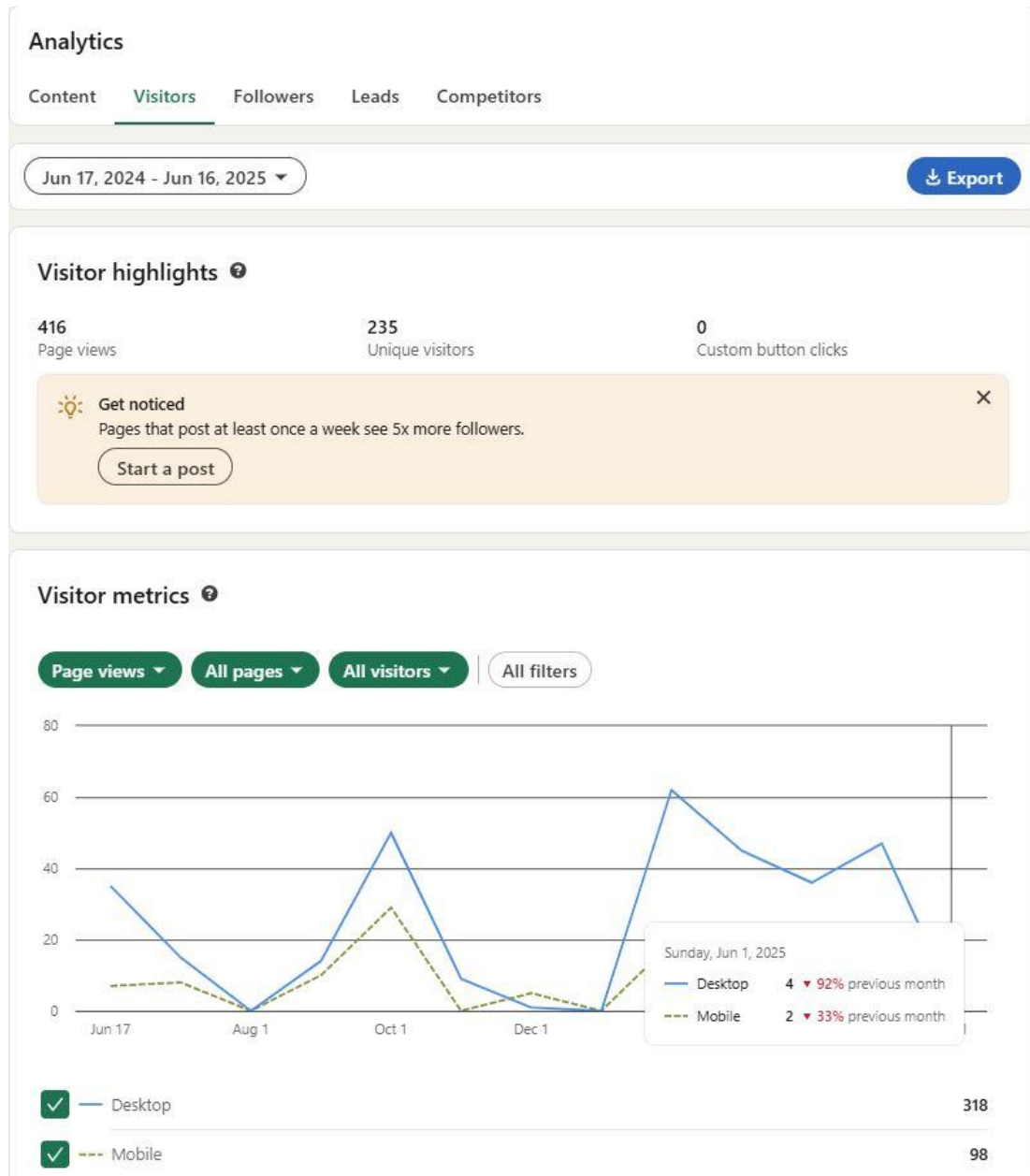


Figure 23. SAND5G LinkedIn metrics for the past year

KPI Satisfaction:

- dKPI-1.1.3 (>10 push announcements and >5 new followers in Twitter/LinkedIn monthly): - **fully satisfied**
- dKPI-1.1.4 (>30 LinkedIn profile views monthly): **> 40 - fully satisfied**
- dKPI-2.1.2 (>10 new discussions per month on LinkedIn): - **fully satisfied**
- dKPI-2.2.2 (>200 YouTube views by end of project): **~ 10 (5%)**

2.2.3 Newsletters

As part of the broader communication strategy, UPAT is responsible for the coordination and publication of the SAND5G project newsletter. The newsletter aims to inform stakeholders about the project's progress, achievements, and upcoming activities in a concise and accessible format. It serves as a complementary channel to the website and social media, targeting both technical and non-technical audiences within and beyond the consortium.

Published Newsletters:

- Issue #1 – September 2024

Highlights:

- Overview of SAND5G goals and project structure
- Description of 5G security challenges and pilot use cases
- Introductory presentation of consortium partners
- Latest submitted deliverables
- Participation in DSD 2024 (Paris)

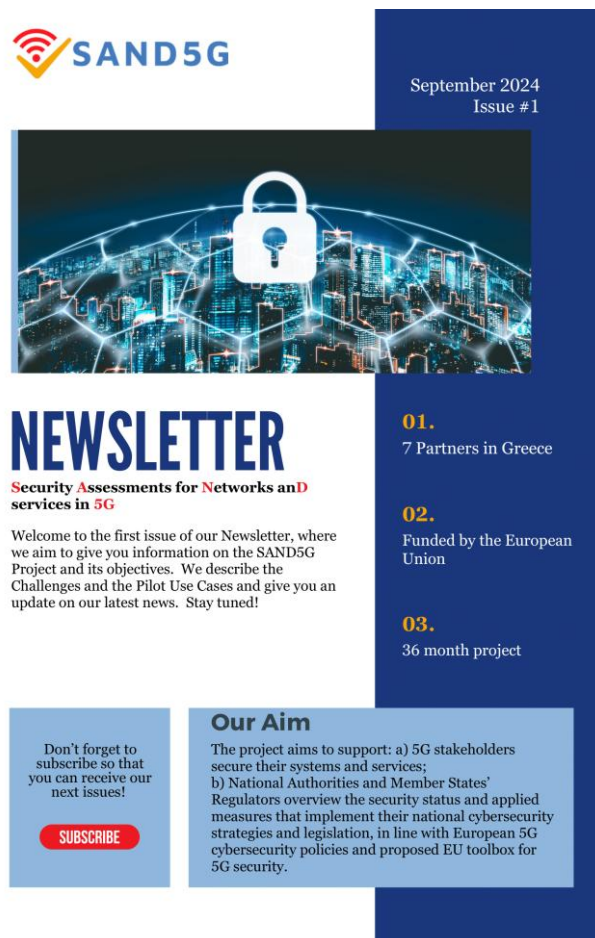


Figure 24. SAND5G 1st Newsletter cover

- Issue #2 – March 2025

Highlights:

- Message from the Project Coordinator (Prof. O. Koufopavlou)
- Plenary meeting in Patras
- Project featured in Phaistos Voice
- Presence at: ETCEI 2024, InfoCom World 2024, Advanced Telecoms & IoT Summit 2024
- Presentation at IEEE CSR 2024



NEWSLETTER

Security Assessments for Networks and
services in 5G



March 2025
Issue #2

A message from
our
Project Coordinator

“
The SAND5G
project is a crucial
initiative for
enhancing the
security of 5G
networks in Europe.

“Welcome to the 2nd edition of the SAND5G Newsletter, where we bring you the latest updates on our progress, highlighting key milestones and advancements in strengthening security and protecting critical infrastructures.

The SAND5G project is a crucial initiative for enhancing the security of 5G networks in Europe. Through the development of a comprehensive risk assessment platform, we aim to support both 5G service providers and national authorities in effectively managing threats and aligning with European cybersecurity policies. This dual approach ensures a cohesive and robust defense mechanism against emerging threats. Our comprehensive deliverables, ranging from in-depth security analyses to targeted training programs, underscore our commitment to excellence and innovation in the realm of 5G cybersecurity.”

*Professor Odysseas Koufopavlou
Project Coordinator
University of Patras*

Figure 25. SAND5G 2nd Newsletter cover

- Issue #3 – April 2025

Highlights:

- Message from Technical Coordinator (Kostas Poullos)
- Sponsorship of IEEE CSR IOSEC Workshop 2025
- 3rd Plenary Meeting in Athens
- Upcoming webinar: “5G Security through the lens of SAND5G” (April 30, 2025)
- Participation in CYSAT 2025 (Paris)
- Announcement of participation at Euromicro DSD/SEAA 2025 (Salerno, Sept 2025)



Figure 26. SAND5G 3rd Newsletter cover

By maintaining a regular newsletter schedule, UPAT contributes to increasing project transparency, strengthening stakeholder engagement, and supporting the dissemination of key results in a user-friendly format. The project remains on track to meet the KPI of issuing at least eight newsletters by the end of the project.

KPI Satisfaction:

- dKPI-1.2.1 (>8 newsletters by end of project): 1 published (April 2025), 1 more scheduled (July 2025) - 37.5% **(3/8)**

2.2.4 Press Releases

UPAT has led the preparation and dissemination of SAND5G press releases, ensuring that major project milestones, events, and achievements are communicated to a wide external audience, including media outlets, research networks, and institutional platforms. Press releases are used as high-impact tools to highlight key developments and raise awareness among non-specialist stakeholders such as policy makers, civil society, and the general public.

The first official press release was issued in M05 to announce the launch of the SAND5G project and introduce its vision, objectives, and consortium partners. It was disseminated through UPAT's institutional website (<https://issg.gr>) and the Patras5G wiki page (<https://wiki.patras5g.eu>), and further shared via LinkedIn and X. The release received positive attention within the Greek cybersecurity and research communities, and helped establish initial visibility for the project.

A second press release is planned for the coming months to highlight the project's midterm progress, with a focus on the first wave of publications, event participations, and platform development. This release is planned for publication around M19 and will be shared through both institutional and project communication channels.

All press releases follow a standardized structure, include visual elements from the project's branding kit, and contain the required EU funding acknowledgments and disclaimers. They are archived in the dedicated *Press Releases* section of the project website to ensure long-term accessibility.

2.2.5 Promotional Material

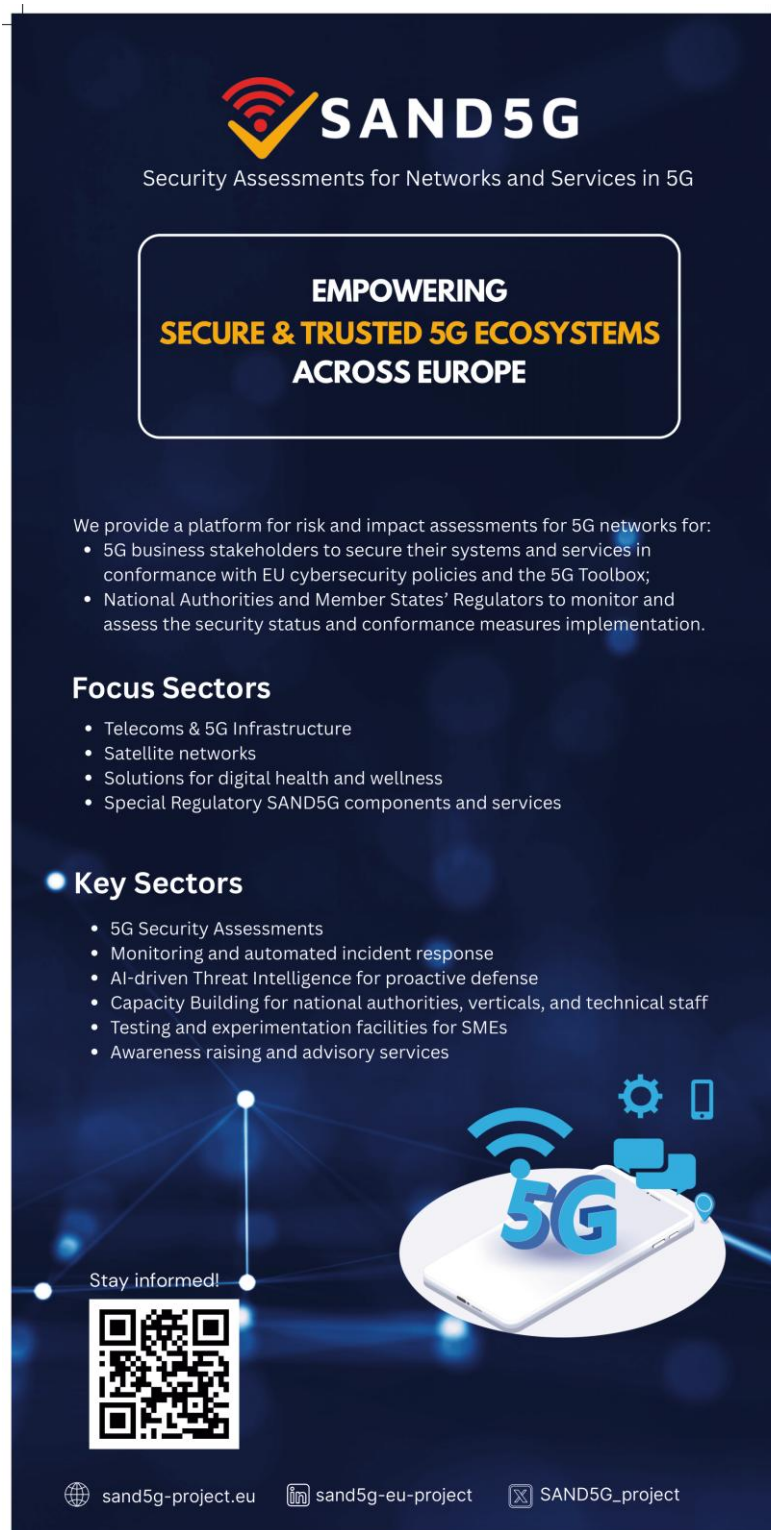
To enhance the visibility and recognition of the SAND5G project, UPAT has developed a comprehensive set of promotional materials aligned with the project's visual identity. These materials include digital and print formats such as banners, leaflets, brochures, and infographics, designed to effectively communicate the project's objectives, key achievements, and partner contributions.



Figure 27. SAND5G brochure



Figure 28. SAND5G brochure



SAND5G
Security Assessments for Networks and Services in 5G

**EMPOWERING
SECURE & TRUSTED 5G ECOSYSTEMS
ACROSS EUROPE**

We provide a platform for risk and impact assessments for 5G networks for:

- 5G business stakeholders to secure their systems and services in conformance with EU cybersecurity policies and the 5G Toolbox;
- National Authorities and Member States' Regulators to monitor and assess the security status and conformance measures implementation.

Focus Sectors




- Telecoms & 5G Infrastructure
- Satellite networks
- Solutions for digital health and wellness
- Special Regulatory SAND5G components and services

Key Sectors

- 5G Security Assessments
- Monitoring and automated incident response
- AI-driven Threat Intelligence for proactive defense
- Capacity Building for national authorities, verticals, and technical staff
- Testing and experimentation facilities for SMEs
- Awareness raising and advisory services

Stay informed!



 sand5g-project.eu  [sand5g-eu-project](https://www.youtube.com/sand5g-eu-project)  SAND5G_project



Funded by the European Union under the Grant Agreement No. 101127979 and supported by the European Cybersecurity Competence Center.

Figure 29. SAND5G pull up banner

Promotional items were utilized during conferences, workshops, and exhibitions to support dissemination activities and facilitate engagement with diverse audiences, including industry stakeholders, researchers, and policy makers. The design approach ensured consistency with the project's branding guidelines, incorporating the official logos, color schemes, and messaging pillars.

In addition to physical materials, UPAT prepared animated and static digital content for online use on social media platforms and the project website, contributing to a cohesive communication ecosystem. Feedback from event participants indicates that the promotional materials have successfully attracted attention and stimulated interest in the project.

Moving forward, UPAT plans to update and expand the promotional portfolio with new content reflecting midterm technical milestones and pilot results. This will include video explainers, enhanced infographics, and translated materials to reach broader international audiences.

KPI Satisfaction:

- dKPI-2.4.1 (>50 hard copies in >5 events): 1 event (TDEX Patras) (16.6%)
- dKPI-2.2.1 (>30 downloads monthly for digital brochures): - **fully satisfied**

2.2.6 Updated Communication Plans

As the SAND5G project evolves, the communication plan has been regularly reviewed and updated to align with emerging project developments, stakeholder feedback, and dissemination KPIs. UPAT led a strategic reassessment of communication objectives and tools at the midterm stage, ensuring that messaging remains relevant and impactful across all target groups.

Key updates to the communication plan include the integration of a more diversified content strategy emphasizing storytelling and use cases to better illustrate the practical benefits of the SAND5G platform. This shift aims to enhance engagement with non-technical stakeholders such as policy makers and industry decision-makers.

Additionally, the plan incorporates new outreach channels, including targeted webinars, interactive social media campaigns, and collaborations with complementary EU projects to amplify project visibility. Efforts to foster community building around cybersecurity and 5G resilience topics have also been prioritized.

UPAT continues to monitor communication metrics closely, leveraging analytics from the website, social media, and newsletter distribution to refine messaging and channel usage. Future updates will focus on scaling activities during the pilot deployment phase and supporting exploitation and sustainability objectives.

KPI Satisfaction:

- dKPI-1.4.1 (3 versions of the CDEB plan): - **Version 1 published; additional updates planned post-pilot phase**
- dKPI-3.3.1 (6 reports published with CDEB KPIs that will be continuously updated throughout the project): 6 reports with CDEB KPI tracking. Status: D5.1 and D5.2 count toward this - **2/6 = ~33%**

2.3 Engagement Approaches and Channels with stakeholders

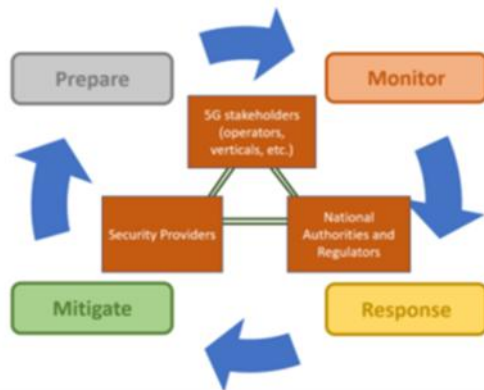


Figure 30. Triangle of Actors collaboration Model

Stakeholder engagement helps to maximize both the contribution of and impact to each of these stakeholders or actors. The project has devised the Triangle of Actors collaboration Model. In the model the three key actor types defined are: 5G (vendors, operators) and verticals stakeholders being the main benefactors of SAND5G work and results, Security Providers and National Authorities and Regulators. The project fosters the creation of a sustainable 5G cybersecurity community of practice, where the identified stakeholder types together with practitioners, researchers, and

educators can share their experiences, insights, and feedback, and collaborate on common issues and solutions.

Stakeholders' engagement involves measuring the engagement level of the different stakeholder types. The following levels of engagement are considered:

- Unaware: Unaware of the issue/solution/ initiative and its potential impacts on them.
- Resistant: Aware of the issue/solution/ initiative yet resistant to change.
- Neutral: Aware of the issue/solution/ initiative yet neither supportive nor resistant.
- Supportive: Aware of the issue/solution/ initiative and supportive of change.
- Leading: Aware of the issue/solution/ initiative and its potential impacts and actively engaged in helping it succeed.

The Stakeholder Matrix depicted in the following Figure provides another useful tool for the engagement process, as it allows positioning of each stakeholder in the matrix, and this will drive the definition of the best engagement approach to be followed for the specific stakeholder. The Stakeholder Matrix combines the level of stakeholder power (authority) and the level of stakeholder interest (concern) for a specific issue, solution, initiative.

POWER	High	Keep satisfied	Manage closely
	Low	Monitor	Keep informed
		Low	High
	INTEREST		

Figure 31. SAND5G Stakeholder Matrix

Based on the analysis above, the main challenge in stakeholders' engagement is the identification and use of the most appropriate and effective channels to foster widespread engagement with the project and maximization of its impact. To the extent applicable, the engagement activity aims to ensure that:

1. All targeted stakeholder types are aware of the project and its approaches and outcomes.
2. The valuable information and services provided by the project reach the intended users.
3. The engagement channels help create awareness, build trust, persuade users to engage with the project and become active members of its ever-growing community and eventually enhance user adoption of the project's results and approaches.

The Stakeholder Engagement Process includes the phases of a./ awareness; b./ co-creation c./ assessment and validation; and d./ adoption. In each phase, different engagement channels are considered most effective and are put into use.



Figure 32. SAND5G Stakeholder engagement process

In the awareness phase, all the Communication channels and tools already described, such as website, social media, newsletters, brochures, project presentations together with surveys and discussions are the most commonly used engagement material and channels and are relevant to all types of stakeholders independently of their disposition, interest or power.

In the co-creation phase, suitable engagement tools include workshops, focus groups or other means to develop R&I agendas, roadmaps and policies, often including scenario building and deep discussion on the implications, ethics, the benefits and the challenges related to R&I courses of action or technology development. Involving citizens and/or end-users directly in the development of new knowledge or innovation, for instance through citizen science and user-led innovation entails the use of surveys, scenario building and design workshops, and focus groups.

In the validation / assessment phase, all stakeholders' active participation, adoption and feedback will ensure optimization of the solutions under pilot experimentation and demonstration. Such participation entails active involvement in Proof of Concepts (PoCs) and pilots, and assisting in the monitoring, evaluation and feedback to the performance, usability, effectiveness of the solution on an iterative or even continual basis. Workshops, surveys, interviews and tests during pilots, and demonstrations will engage representatives of targeted communities.

For the take-up phase and to support and strengthen the adoption, open documentation (such as factsheets, report briefings and white papers) as well as publications and active participation and contributions / presentations to public dissemination events such as conferences, exhibitions, trade fairs constitute the most appropriate engagement channels to be employed.

3 Exploitation & Sustainability Activities

3.1 Partners' Individual Exploitation Plans

UPAT		
Role in the Project	Expectations from the Project	Exploitation Plan
UPAT has multiple roles in the project. Firstly, it is responsible for the overall management of the project and consortium, including the management of legal, financial, and administrative duties, as well as the quality management procedures that will be followed throughout the project (WP1). Additionally, UPAT provides one of the key pilot to validate the SAND5G proposed system. It offers its 5G infrastructure, an isolated Non-Public Network used for testing and experimentation of 5G and IoT applications. Furthermore, it is responsible for defining the trial scenarios and specifying the evaluation methodology for the project (T4.1). Finally, UPAT is responsible of the final report on Dissemination, Exploitation, Standardization, and Sustainability (T5.3).	UPAT is leading the development of an educational tool designed to provide high-quality cybersecurity training. By combining its expertise in education with that of consortium partners, it creates specialized cybersecurity courses. In addition to its educational initiatives, UPAT is responsible for the validation and pilot testing of SAND5G using its 5G infrastructure. By integrating SAND5G with 5G technology, UPAT will assess its usability, cybersecurity capabilities, and integration complexity. This pilot is a critical step in demonstrating SAND5G's ability to operate securely within various environments while ensuring compliance with strict security requirements. With extensive experience in developing and managing secure systems, UPAT is well-positioned to lead this effort. Throughout the validation process, it will provide continuous feedback to the consortium, optimizing deployment scenarios and addressing key integration challenges. By advancing both cybersecurity education and secure system validation, UPAT strengthens its role as a leader in bridging academia with industry while driving innovation in cybersecurity solutions.	UPAT is highly interested in participating in a joint exploitation strategy for the SAND5G platform, with a particular focus on developing research papers and educational materials. As an academic institution, UPAT's contribution will primarily involve creating high-quality content to support the platform's adoption and use in educational and research contexts. Furthermore, UPAT validates the SAND5G platform's usability and effectiveness in on-premises environments through its 5G infrastructure pilot, demonstrating the platform's value for organizations requiring high-security, on-premises solutions. In addition, UPAT will deploy training courses and workshops with main scope to attract collaborations with industry partners, offering real-world training modules developed by consortium members.

Table 1. UPAT Exploitation Plan

SPH		
Role in the Project	Expectations from the Project	Exploitation Plan
<p>SPH leads (WP3) "Development of SAND5G platform for 5G and beyond networks and services" and is responsible for defining the (T2.3)"SAND5G platform design and technical specifications", while also acting as the (T1.2) Technical Coordinator. In addition, we contribute to (WP5) "Communication, Dissemination, Exploitation and Standardization Activities" as well as leading on (T3.2) "Development SAND5G platform for 5G networks and services—First prototype" and (T4.4) "Refinements towards the final SAND5G platform for 5G networks and services – Final release". As a dedicated cybersecurity provider, SPH implements a solution where national authorities author playbooks and SAND5G executes them according to plan, ensuring a secure-by-design infrastructure throughout the project.</p>	<p>SPH expects the project to drive the advancement of secure 5G and beyond network technologies by validating SPH's cybersecurity solution in 5G space. SPH's cooperation with consortium partners provides a great opportunity for enhancing SPH's CACAO-playbook driven approach, ensuring that our integrated security measures align with the highest industry standards. The priority to optimize our system's usability, resilience, and of course scalability, is served through pilot testing and continuous technical feedback. This process is anticipated not only to enhance the performance of the SAND5G platform but to help SPH's position as an innovator in cybersecurity solutions and connect SPH's systems with new and interesting use cases.</p>	<p>SPH's exploitation strategy focuses on maximizing the impact of SPH's cybersecurity framework within the SAND5G platform. SPH's goal is to disseminate scientific knowledge, technical papers, and best practices that highlight the essence of SPH's CACAO-playbook approach. Additionally, SPH plans to organize training workshops and live demonstrations to engage industry partners and standardization bodies, by demonstrating the robustness and adaptability of our solution. Through the employment of the project outcomes, SPH is aiming to establish a leading role in the market and promote the broader adoption of advanced cybersecurity measures for next-generation networks.</p>

Table 2. SPH Exploitation Plan

p-NET		
Role in the Project	Expectations from the Project	Exploitation Plan
<p>P-NET's main role in SAND5G is to orchestrate the Knowledge and Capacity Building activity (Lead beneficiary of Task T3.3) which targets at improving the skills, awareness, collaboration of the overall EU 5G ecosystem. Training activities and material will be designed and developed and will be specialized on the one hand towards vertical services stakeholders and the general public and on the other hand towards technical personnel of 5G infrastructures and relevant National Authorities. P-NET is also the lead beneficiary of Task T5.2 on Impact creation, exploitation and standardization activities.</p>	<p>P-NET is a Competence Centre for Emerging Smart Networks and Services. Its operations and services are centered around knowledge and technology transfer and include research and development of business solutions, experimentation and pilot testing in advanced lab infrastructure and experimental facilities, upskilling and reskilling training on topics relevant to telecoms and the element of smartness in networks and services. The Centre also aims to create awareness and offer consulting services to public authorities and businesses and mentoring start-ups. SAND5G activities and results cut across and are relevant to all services and operations of the Competence Centre.</p>	<p>P-NET's exploitation roadmap is multi-dimensional and refers to a./ extending the Centre's competence on the topic of cybersecurity certification; b./ expand and enrich our experimental facility and capabilities in secure Beyond 5G and 6G systems; c./ pursue collaborative R&I activity and engage with SAND5G partners in preparing and submitting relevant follow-up proposals and raising additional R&I funding; d./ creating training content and/or designing and delivering webinars thus enriching p-NET's relevant capacity building activity; 5./ building strong partnerships with potential for joint business development.</p>

Table 3. p-NET Exploitation Plan

WINGS		
Role in the Project	Expectations from the Project	Exploitation Plan
<p>WINGS main role in the project is related to the Health Vertical service to be provided as one of the pilots. As such, WINGS participates in WP2 "SAND5G Requirements and Architecture specification" activities in terms of pilot user needs, requirements, technical specifications and architecture design; WP3 "Development of SAND5G platform for 5G and beyond networks and services" in terms of necessary APIs between the SAND5G tools and the Health platform as well as related adaptations needed to this end in the Health platform; WP4 "Validation activities and refinements towards deployment in operational environments" in the context of setting up the Health pilot per se as well as validating the SAND5G tools in this case; and WP5 "Communication, Dissemination, Exploitation and Standardization Activities" for communicating the outcomes of the project and bringing them closer to the market.</p>	<p>Security is critical for all WINGS products. In the case of remote health monitoring in particular, it is of paramount importance to ensure data privacy of the people in need and that only personnel with the correct authorization can access them. Security risks and vulnerabilities posed by either IoT devices or the 5G infrastructure per se need to be assessed both at set-up as well as continuously due to the sensitivity of these data.</p>	<p>WINGS is always interested in participating in projects that can enhance the products of its portfolio or provide the opportunities to identify new needs in the market. Within SAND5G, we envision the identification of further enhancements for our wi.CARE+ (previously called STARLIT) platform in terms of security as well as connectivity through 5G infrastructures. The enhancements of wi.CARE+ will accordingly be integrated in our portfolio and eventually released in the market.</p>

Table 4. WINGS Exploitation Plan

OQ Technology		
Role in the Project	Expectations from the Project	Exploitation Plan
<p>OQ Technology main role in the SAND5G project is to provide a pilot that is related to the Space Vertical Service. To achieve that, OQ Technology participates in WP2 to provide user requirements, and functional and non-functional requirements for the pilot.</p> <p>Also participates in WP3 to provide the bridge between the Space Vertical Service and SAND5G platform. Furthermore, participates in WP4 to set up the necessary architecture and technologies so the SAND5G tools can be validated.</p> <p>Finally, as part of WP5, OQ Technology plans to communicate the project purpose and outcomes to the audience that is directly working with.</p>	<p>As OQ Technology expands the space operations, it is crucial to fortify even better the security of non-terrestrial networks that are linked to satellite and IOT communications over 5G.</p> <p>With the use of SAND5G platform there is the opportunity to assess any security risks and vulnerabilities that might emerge and take action to mitigate risks from relevant threats.</p>	<p>OQ Technology, being a LEO satellite operator and the world's first LEO 5G IoT satcom company, offers global IoT satcom solutions.</p> <p>Collaborating in a joint exploitation strategy for the SAND-5G platform is of critical importance.</p> <p>First as a satcom operator it is vital to contribute in solutions for the enhancement of (cyber)security & connectivity protocols which can be integrated to OQs already existing satellite constellation thus strengthening its security and connectivity protocols.</p> <p>Furthermore, as OQ technology has offices in Greece (OQ Technology Hellas), it is also important to expand the team by attracting new talents thus also contributing in the development of the Greek space sector with new jobs.</p> <p>Participating in this project also strengthens collaboration opportunities with other Greek companies and academia.</p>

Table 5. OQ Technology Exploitation Plan

ADAE		
Role in the Project	Expectations from the Project	Exploitation Plan
ADAE (Hellenic Authority for Communication Security and Privacy) leads Work Package 2 "SAND5G Requirements and Architecture specification" and is responsible for "Security analysis for 5G and beyond networks" (D2.1). ADAE provides the perspective of National Authorities and Regulators in the project, contributing to requirements definition and piloting activities. The organization also plays a key role in helping implement the EU 5G Toolbox and national strategies for 5G security.	ADAE expects the SAND5G platform to provide tools that will enable National Authorities to monitor the security status of 5G infrastructures and services within their jurisdiction. The platform should facilitate the enforcement of EU and national regulations and legislation. ADAE anticipates using SAND5G to access tools for creating reporting playbooks that implement specific practices and processes according to national strategies.	ADAE plans to utilize the SAND5G platform to enhance its monitoring and enforcement capabilities related to 5G security. The Authority aims to leverage the platform to gain better oversight of security measures implemented across 5G networks and services in Greece. ADAE will use the knowledge and tools developed in the project to improve regulatory processes and coordination with operators and service providers. The authority also intends to develop connections with other EU regulators and agencies to share best practices in 5G security enforcement.

Table 6. ADAE Exploitation Plan

NCSA		
Role in the Project	Expectations from the Project	Exploitation Plan
<p>NCSA's main role in the project is the lead beneficiary in the task 5.3 "Stakeholder, EC, and National Authorities Engagement" of WP5 "Communication, Dissemination, Exploitation and Standardization Activities". This task involves contribution of information, by all partners, about their national and international links and their engagement for strategic collaborations with businesses, vertical industries and public authorities that can benefit and/or add value to the project. Through this task, SAND5G will prepare a database of external institutional and domain-focused stakeholders and will perform constant interactions, based on the existing cooperation. The scope is to raise the awareness of SAND5G project as a major referral point when implementing the security dimension over the 5G technologies, infrastructures and services.</p>	<p>The National Cybersecurity Authority (NSCA) of Greece aims to organize, coordinate and implement a comprehensive framework of strategies, measures and actions for achieving and maintaining a high level of prevention, protection, deterrence, response and recovery from cyberattacks. It is the competent Authority for monitoring and supervising the implementation of the European Union's Directive on measures for a high common level of cybersecurity across the Union – NIS2. NCSA fulfills a multidimensional role in enhancing cybersecurity, ensuring the protection of national digital infrastructures and promoting a secure and innovative digital ecosystem, acting as a cybersecurity supervisory and coordinating mechanism. In this context, the SAND5G platform, through its training, detection, analysis, protection and response capabilities will play a crucial role in achieving a high level of cybersecurity for 5G entities and thus fulfilling the most important expectation of NCSA.</p>	<p>Within SAND5G, NCSA's exploitation plan involves gaining continuous insights, statistics and situational awareness about the cybersecurity of the Greek 5G ecosystem and thus contributing to the formulation of its overall public policy concerning national digital infrastructures. NCSA is also highly interested in supporting innovation, scientific research and investments in cybersecurity and promoting education and awareness in the field. To this end, the SAND5G platform will help NCSA develop collaborations with public, private, academic and research institutions.</p>

Table 7. NCSA Exploitation Plan

3.2 SAND5G Exploitation Process

At this stage the project is midway through its lifetime and discussions within the partnership have been initiated on the Exploitation potential that is being created with the view to defining proper exploitation roadmaps for the project results. The process to be followed towards this end involves:

1. The definition and characterization of anticipated Project Results.
2. The identification of the project's Key Exploitable Results (KERs).
3. The definition of the Go-to-Market Roadmap of each of the identified KERs.

For completeness, we give below the definitions of Results and Key Exploitable Results as used in the present section and in the project.

Result: "Any tangible or intangible output of the action, such as data, knowledge and information whatever their form or nature (including software and hardware), whether or not they can be protected, which are generated in the action".

KER: "Main interesting result (as defined above) which has been selected and prioritised due to its high potential to be 'exploited' downstream the value chain of a product, process or solution, or act as an important input to policy, further research or education".

In the following we detail the work to be performed in each one of the three steps of the exploitation process.

3.2.1 Characterization of Project Results

Partners' views on anticipated project results, as viewed from the perspective of each partner's role and contribution in the project will be collected with the use of the following template (a shortened version of the Characterization Table proposed by the HORISON RESULTS BOOSTER Services).

Name of Result	
Partner - Owner	
Description	
Problem	<p><i>Describe the problem addressed (the problem your potential users have).</i></p> <p><i>Potential users are the people, companies, organisations, etc. that you expect will use the result (and generate an impact). They are your "Customers".</i></p>
Alternative solution	<p><i>Describe how your "customer" has solved the problem so far.</i></p>
Unique Selling Point USP - Unique Value Proposition UVP	<p><i>Describe the competitive advantages, the innovative aspects. What does your solution do better, what are the benefits considering what your user/customer wants, how does your solution solve his/her problem better than alternative solutions, what distinguishes the Result from the competition / current solutions?</i></p>

"Market" – Target market	<p><i>Describe the market in which your product/service will be used/can "compete", answering the following questions:</i></p> <ul style="list-style-type: none"> - <i>What is the target market?</i> - <i>Who are the customer segments?</i>
"Market" - Competitors	<p><i>Who are your "competitors" (note: they are the ones offering "alternative solutions")?</i></p> <p><i>What are their strengths and weaknesses comparing to you?</i></p>
Use model	<p><i>Explain what is your "use model", how the Result will be put in use (made available to "customers" to generate an impact). Examples of use models: manufacturing of a new product, provision of a service, direct industrial use, technology transfer, license agreement, contract research, publications, standards, etc.</i></p> <p><i>Note training is a service.</i></p>
IPR Status	<p><i>What is the Background (type / partner) & the Foreground (type / partner)?</i></p> <p><i>Provide information considering also what already agreed in the Consortium Agreement and in Annex I.</i></p>

Table 8. Template of Characterization Table

3.2.2 Identification of Key Exploitable Results (KERs)

The collected material will be studied, discussed and analysed by the project's Innovation Management Committee (IMC). The Committee is formed by the Innovation Manager (IM) plus one representative of each Beneficiary who is close to the business and aware of market trends. The mandate of IMC is to monitor actual market needs and evaluate the identified project results with regards to their exploitation potential vis-à-vis emerging innovation needs in the sector.

The Committee will continuously analyse the technical progress of the project and the state of the art in the market and be responsible for the selection of the project's Key Exploitable Results (KERs).

3.2.3 Go-to-Market Roadmap

Main exploitation aspects of the identified Key Exploitable Results are that they:

- ✓ Respond to specific needs of a well-defined group, the "adopters".
- ✓ Solve their need/s much better than "state of the art".
- ✓ Are chosen by partner/s for commercial or not-for-profit use and/or "market" introduction.

For the definition of the Go-to-Market Strategy for each one of them the project will use a number of Tools including the Market Definition Canvas, the Value Proposition Canvas and the Lean Canvas, possibly with the support of the Booster Services offered by the European Commission.

The Market Definition Canvas is a strategic tool, primarily developed by Tony Ulwick of Strategyn, that helps organizations define their market through the lens of Jobs-to-be-Done (JTBD).

Instead of focusing on products or customer demographics, it shifts the focus to:

- The "Job Executor": The specific group of people who are trying to get a job done.
- The "Job-to-be-Done": The core functional task or problem that these people are trying to accomplish or solve, often regardless of the specific product they might use.

By using this canvas, businesses can gain a deeper understanding of their customers' underlying needs, leading to more targeted innovation and competitive differentiation. It is designed to provide a stable definition of the market that remains relevant even as products evolve.

The Value Proposition Canvas, developed by Alex Osterwalder (also the creator of the Business Model Canvas), is a framework used to design, evaluate, and refine the value proposition of a product or service to ensure it aligns with customer needs.

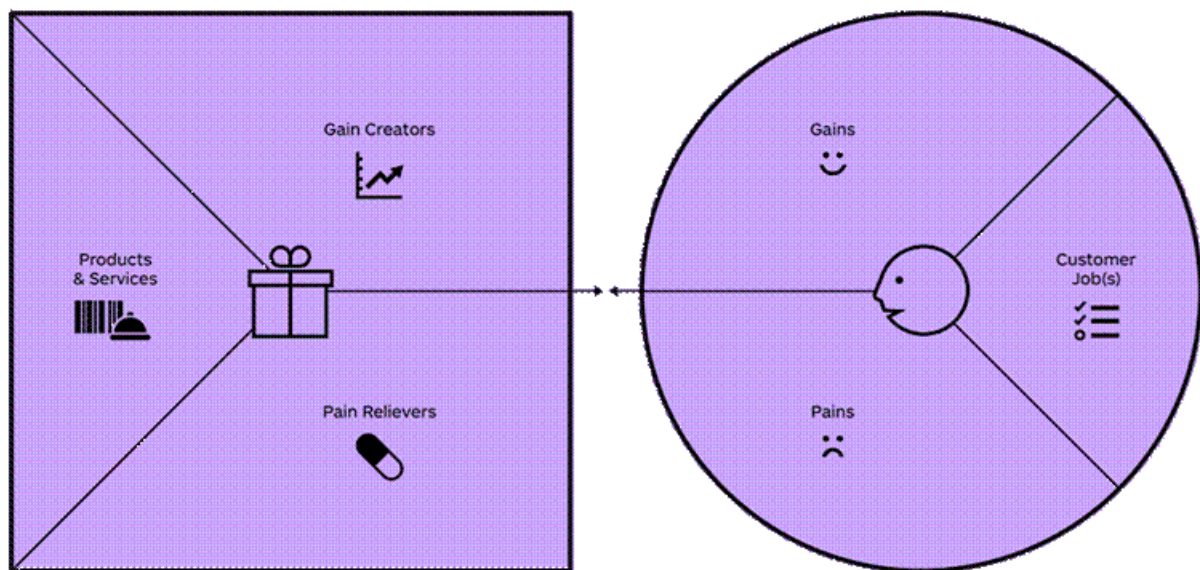


Figure 33. Value Proposition Canvas

It consists of two main parts:

1. **Customer Profile** (Right Side - Circle): This section details the target customer, focusing on:
 - **Customer Jobs:** The functional, social, and emotional tasks or problems the customer is trying to get done.
 - **Pains:** The negative experiences, emotions, or risks the customer encounters while trying to get their jobs done.
 - **Gains:** The positive outcomes, benefits, or desires the customer expects or would be delighted by.
2. **Value Map** (Left Side - Square): This section describes the product or service offering, focusing on:
 - **Products & Services:** A list of what you offer.
 - **Pain Relievers:** How your products/services specifically alleviate customer pains.
 - **Gain Creators:** How your products/services create gains for the customer.

The goal of the Value Proposition Canvas is to achieve "fit" between the customer profile and the value map, meaning your products and services effectively address the most important customer pains and create significant gains. This helps businesses create offerings that truly resonate with their target market and achieve product-market fit.

The Lean Canvas is a one-page business plan template created by Ash Maurya, adapted from Alex Osterwalder's Business Model Canvas. It's specifically optimized for startups and new ventures, prioritizing agility and problem-solving.

Instead of an exhaustive traditional business plan, the Lean Canvas focuses on key assumptions and hypotheses that need to be validated, making it ideal for the iterative "Lean Startup" methodology. Its nine blocks typically include:

- **Problem:** The top problems your customers face.
- **Customer Segments:** Who experiences these problems.
- **Unique Value Proposition (UVP):** What makes your solution different and worth buying.
- **Solution:** Your proposed way to solve the identified problems.
- **Channels:** How you'll reach your customers.
- **Revenue Streams:** How your business will make money.
- **Cost Structure:** The expenses involved in running your business.
- **Key Metrics:** How you'll measure success and progress.
- **Unfair Advantage:** Something you have that can't be easily copied or bought.

The Lean Canvas encourages entrepreneurs to quickly sketch out their business idea, identify the riskiest assumptions, and then test and iterate based on real-world feedback.

4 Clustering and Standardization

4.1 Clustering Activities and Plans

4.1.1 Clustering Objectives

Clustering in EU projects involves strategic coordination between related initiatives to maximize impact and efficiency. For SAND5G, this includes identifying projects with similar focus on 5G security, cybersecurity infrastructure protection, and digital trust, while establishing structured collaboration frameworks within the DIGITAL-ECCC-2022-CYBER call ecosystem and broader cybersecurity community.

The SAND5G clustering strategy encompasses joint activities such as coordinated events, shared meetings, and collaborative actions that leverage complementary expertise and resources across projects working on 5G security, network protection, and cybersecurity capacity building.

SAND5G's clustering objectives are clearly defined to achieve specific outcomes in knowledge sharing, resource optimization, market impact, and standardization, particularly focusing on the implementation of the EU 5G Toolbox and supporting National Authorities in cybersecurity enforcement.

Clustering is prioritized in SAND5G to achieve the following key objectives aligned with our project's mission to deliver a risk and impact assessment platform for 5G networks:

Technical synergies in 5G security and cybersecurity

Technical synergies represent the strategic alignment and integration of 5G security capabilities, cybersecurity knowledge, and risk assessment resources across multiple projects to create greater collective value than individual efforts could achieve alone. These synergies are particularly important given SAND5G's focus on implementing the EU 5G Toolbox measures and supporting National Authorities.

To achieve technical synergies, we will establish a structured knowledge exchange framework via regular technical workshops focusing on 5G security architectures, CACAO playbook implementations, and cybersecurity risk assessment methodologies. Anticipated technical synergies could involve systematic resource sharing of security datasets, 5G testing environments (leveraging UPAT's 5G infrastructure), threat intelligence feeds, and collaborative security assessment procedures.

Innovation ecosystem for 5G and cybersecurity

To become part of the larger 5G and cybersecurity innovation ecosystem, SAND5G will establish strategic partnerships with key stakeholders including research institutions specializing in 5G security, industry players in telecommunications and cybersecurity, National Cybersecurity Authorities, and technology transfer offices. This involves creating a structured framework for knowledge exchange around the SAND5G platform and joint development activities in 5G security solutions.

Our activities will focus on organizing a series of webinars on 5G security topics, facilitating technology transfer sessions for the SAND5G platform, and developing joint exploitation strategies with partners like SPH, WINGS, and OQTECH. We will establish clear mechanisms for intellectual property management and commercialization pathways for 5G security solutions, ensuring that innovations can effectively move from research to market implementation in the cybersecurity sector.

Policy alignment with EU 5G cybersecurity strategy

SAND5G supports the European Commission's collaborative approach by aligning outcomes with EU policy priorities, particularly the EU 5G Toolbox implementation and National Cybersecurity

Authorities' requirements. We engage with policymakers, participate in policy discussions through our National Authority partners (ADAE and NCSA), and provide evidence-based recommendations to inform decision-making on 5G security policies.

We will establish regular policy engagement through workshops and consultations, leveraging our consortium's direct connections with Greek National Authorities and European cybersecurity networks. This includes creating policy briefs based on SAND5G platform findings and participating in expert groups to share our findings on 5G security risk assessment and contribute to policy development in cybersecurity and telecommunications security.

Communication amplification in cybersecurity and 5G communities

Strategic partnerships and collaborations with other cybersecurity and 5G security projects create valuable opportunities for enhanced dissemination and communication efforts. By joining forces with complementary initiatives focusing on network security, digital infrastructure protection, and cybersecurity capacity building, we can amplify our message through shared channels and platforms, reaching stakeholders across telecommunications, vertical industries, and regulatory bodies.

Through these partnerships, we can develop targeted communication strategies that address specific audience segments including 5G operators, vertical service providers (health, space, manufacturing), National Authorities, and cybersecurity professionals. By leveraging the combined networks and expertise of multiple projects, we can create more compelling narratives around 5G security and deliver them through optimized channels within the cybersecurity and telecommunications communities.

4.1.2 Project Landscape Mapping

Project Landscape Mapping for SAND5G involves a thorough examination and evaluation of various research initiatives that align with our project's objectives in 5G security, cybersecurity infrastructure protection, and digital trust. This process encompasses EU-funded projects under the [DIGITAL-ECCC-2022-CYBER call](#), related Horizon Europe cybersecurity projects, national research programs in Greece and other EU Member States, and industry initiatives that address similar challenges in 5G security and network protection.

The mapping extends across different framework programs, including Horizon Europe's Cluster 3 (Civil Security for Society), Digital Europe Programme cybersecurity actions, and previous Horizon 2020 cybersecurity projects, to identify projects with shared goals in 5G security, cybersecurity technologies, or telecommunications protection.

4.1.3 EU-Funded Projects

4.1.3.1 Projects from DIGITAL-ECCC-2022-CYBER Call

We conduct thorough analyses of all projects funded under the DIGITAL-ECCC-2022-CYBER call, particularly those addressing Topic DIGITAL-ECCC-2022-CYBER-03 focusing on 5G infrastructure security. This comprehensive mapping helps us identify immediate opportunities for collaboration with sister projects working on similar 5G security challenges, cybersecurity capacity building, or National Authority support systems. For example, 5G-Tactic project has been already invited to participate in the panel of a webinar organised by p-NET for SAND5G, and a follow-up webinar is organised by p-NET with the support of both SAND5G and 5G-Tactic projects.

Based on this analysis, we establish regular engagement with these sister projects through dedicated clustering activities, ensuring effective coordination and knowledge sharing across the call, particularly in areas of 5G security assessment, cybersecurity training, and regulatory compliance support.

4.1.3.2 Related EU Projects and Cross-Program Analysis

We leverage our partners' existing networks and collaborations to identify related projects. Each SAND5G partner takes the lead in establishing and maintaining relationships with projects they are already connected to:

- UPAT focuses on projects where they have involvement through CONCORDIA (European Cybersecurity Competence Centre pilot) and other cybersecurity initiatives
- SPH engages with projects utilizing their cybersecurity frameworks and CACAO playbook implementations
- UPAT connects with 5G testing and validation projects through their 5G infrastructure networks
- ADAE and NCSA will engage with regulatory and policy-focused projects involving National Authorities
- WINGS connects with health sector cybersecurity and IoT security projects
- PNET focuses on 5G competence building and 5G testing and experimentation facilities and services
- OQTECH engages with space and satellite communication security projects

Our partners focus on projects within Horizon Europe's Cluster 3, Digital Europe Programme, and relevant Horizon 2020 continuation projects, particularly those addressing cybersecurity, 5G security, critical infrastructure protection, and digital trust.

Project / Initiative	Scope Description	Link	Forms of collaboration	Partner Responsible	Progress Made
5G-TACTIC	5G-TACTIC focuses on 5G networks Cybersecurity and Trust and brings together National Regulation Authorities from 3 EU Members States and Cybersecurity Authorities from 3 Member States, technology innovating European SMEs developing Open 5G solutions and security services, infrastructure providers & mobile network operators. These	https://www.5g-tactic.eu/	Sister project, exchange of results and best practices, co-organization of events	p-NET	Co-organization of Webinar#2 planned for July 2, 2025. The theme of the webinar is "Cross-border Cybersecurity through the Lens of Government"

	will collaborate with research & academic institutes to develop secure, open, disaggregated & interoperable 5G solutions to support an open & competitive 5G European ecosystem.				
Phoeni2x	A Cyber Resilience Framework providing Artificial Intelligence (AI) – assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange, tailored to the needs of Operators of Essential Services (OES) and of the EU Member State (MS) National Authorities entrusted with cybersecurity.	https://phoeni2x.eu/	UPAT participation (coordinator). Writing papers with researcher of this project	UPAT	
CUSTODES	A Certification approach for dynamic, agile and reUSable assessment fOr composite systems of ICT proDucts, servicEs, and processeS	https://custodes-project.eu/	P-NET participation Organizing joint workshops/conf erence special sessions	P-NET	TEDx Event in Patras: the training event organized by SAND5G was supported by CUSTODES. Planning of joint co-creation event at Techritory 2025, in October 2025.
CONSOLE	Cybersecurity for Resilient Software Development - Boosting cybersecurity in the EU software development sector with an automated, unified	https://console-project.eu/	UPAT participation. Writing papers. Writing papers with researcher of this project	UPAT	

	platform of tools and services				
FIDAL	FIDAL is a research project focused on improving 5G networks and preparing for future 6G technology. They're building test labs and creating tools to make networks smarter and more automated, with a special focus on media services and emergency response systems. The project also allows other companies to test their own ideas using FIDAL's facilities.	https://fidal-he.eu	UPAT participation P-NET participation Writing papers with researcher of this project Organizing workshops/conference special sessions	UPAT/p-NET	
ACROSS	ACROSS is a HORIZON-JU-SNS-2022 funded research project that designs and implements an end-to-end service deployment and management platform for next generation networks and services, aiming at unprecedented levels of automation, performance, scalability, and energy efficiency.	https://across-he.eu	UPAT participation p-NET participation Writing papers with researcher of this project	UPAT/p-NET	
NATWORK	The NATWORK project aims to develop a novel AI-leveraged self-adaptive security mechanism for 6G networks based on resilient bio-mimicry principles. The goal is to improve the malleability and the self-resilience of future 6G network ecosystems to offer augmented and secure	https://network-project.eu/	Joint organization of events. Participation in each other's events	p-NET	NATWORK's coordinator was a panelist in SAND5G webinar #1 Both projects will be involved in the Cybersecurity co-creation event organised by p-NET in the Techritory Forum 2025

	services at the lowest energy costs.				
P2CODE	The P2CODE project aims at innovating and creating a wide-open, secure and trusted IoT-to-edge-to-cloud compute continuum that will realize the true potentials of edge intelligence.	https://p2code-project.eu	UPAT participation Writing papers with researcher of this project.	UPAT	
CURIUM	CURIUM project aims to support the implementation of CRA and enhance the resilience, security, privacy, and accountability of all hardware and software products with digital elements, through the design and development of a novel Compliance Continuum provided via a set of cybersecurity-oriented tools and services offering information, guidance, trustworthy Security Testing and essential requirements fulfilment facilitation.		p-NET participation Organization of joint events	p-NET	TEDx Event in Patras: the training event organized by SAND5G was supported by CURIUM. Planning of joint co-creation event at Techritory 2025, in October 2025.
CONFIDENTIAL6G Confidential Computing and Privacy-preserving Technologies for 6G	The project aims at ensuring reliability, trust and resilience for 6G infrastructures that integrates emerging AI tools, new hardware components and accelerators, compute and networking functions, IoT and edge nodes. It emphasizes on privacy preservation and security of sensitive data by focusing on protection of data: a) In use; b) In	https://confidential6g.eu/	WINGS is the coordinator of the project and can support the interaction between the 2 projects for either commonly organized events or for knowledge transfer	WINGS	

	transit; and c) At the Edge.		between the 2 projects.		
RIGOUROUS security design and deployment of trustworthy continuous computing 6G Services	The project aims to improve the security, privacy and trust present in both 6G and other novel computing technologies and services. To do so, it will develop an innovative smart service framework that will make software and AI parts comply with security requirements throughout their development and up to launch while detecting and stopping security breaches. The project is also researching possibilities to improve the secure and efficient automation of security management.	https://rigorous.eu/	WINGS, as a project partner, will support the knowledge transfer between the 2 projects.	WINGS	
AMAZING 6G	AMAZING-6G proposes 14 use cases in the fields of healthcare, public safety, energy, and transportation (including rail transport), which will be presented in large-scale, Europe-wide trials. Innovative technologies are expected to be developed and tested in the following areas: Communications, Compute-as-a-Service, Applications and AI, IoT and Location.	AMAZING 6G - European Projects of the City of Torino	WINGS coordination	OQ, p-NET	

Table 9. SAND5G partners' participation in other EU projects

4.1.3.3 Industry Programs and Clusters

We conduct a comprehensive analysis of industry programs and private sector clusters relevant to 5G security and cybersecurity, focusing on:

- GSMA Security Working Groups (through ADAE's participation in GSMA Fraud and Security Group)
- ENISA cybersecurity initiatives and network security programs
- 6G-IA (6G Smart Networks and Services Industry Association) activities (UPAT and p-NET are already members and active contributors)
- ECSO (European Cyber Security Organisation) initiatives
- 5G-PPP security working groups and related industry clusters
- National cybersecurity industry associations and competence centres

Through this process, we develop targeted engagement strategies to establish meaningful collaborations with private sector stakeholders while ensuring compliance with all relevant participation requirements and constraints, particularly leveraging our partners' existing industry connections.

4.1.4 Clustering Activities & Methodology

4.1.4.1 Joint Webinars & Events

Joint webinars and events serve as the cornerstone of SAND5G's clustering strategy, providing structured opportunities for knowledge exchange and collaboration in 5G security, cybersecurity frameworks, and regulatory compliance support.

Regular 5G Security Webinars through the lens of [government, technology, innovation etc]

SAND5G organizes a series of webinars with sister projects and related cybersecurity projects. These gatherings are conducted virtually (90-minute sessions) or in-person (full-day meetings) and focus on:

- SAND5G platform demonstrations and technical deep dives
- 5G security methodologies and best practices sharing
- EU 5G Toolbox implementation experiences and lessons learned
- CACAO playbook development and standardization efforts
- National Authority requirements and regulatory compliance approaches
- Cybersecurity training program development and sharing

4.2 Standardization Activities and Plans

4.2.1 Goals for standardization and a strategic framework

SAND5G's plan for standardization is in line with the goals of the European Commission's Digital Single Market and the use of the EU 5G Toolbox. Our standardization work directly helps set up consistent cybersecurity standards across all EU Member States, especially when it comes to National Authority requirements and regulatory compliance frameworks. This is because our project is focused on security assessments for 5G networks and services.

The project's goals for standardization are to make the most of the SAND5G platform's features while making sure they are in line with current and future European cybersecurity standards, 5G security frameworks, and rules set by ENISA, ETSI, and other relevant standardization bodies.

4.2.1.1 *Main Goals of Standardization*

Harmonization of the 5G Security Framework SAND5G's

This goal helps 5G security assessment methods be more consistent across the European Union. It does this by expanding on the work done by the EU 5G Toolbox and helping National Authorities use the same security review methodology. Our work will mainly be about creating standardized methods for risk assessment, threat analysis, and security monitoring that may be used by telecom operators, vertical service providers, and regulatory agencies.

We will make recommendations for security assessment protocols based on evidence that can be added to existing ETSI, 3GPP, and ENISA frameworks through our platform development and pilot validation activities. This will make sure that different implementation environments and jurisdictions can work together and stay consistent.

Standardization of Cybersecurity Playbooks SAND5G

This will help make automated cybersecurity response procedures more consistent for 5G networks by building on SPH's experience in creating CACAO (Collaborative Automated Course of Action Operations) playbooks. This includes creating standardized playbook templates, response protocols, and integration interfaces that can be used on a variety of cybersecurity platforms and National Authority frameworks.

Our main goal is to create standardized ways to automate incident response, share threat intelligence, and coordinate security activities that are in line with European cybersecurity plans and help meet the criteria of the NIS2 Directive.

Standards for Compliance with Regulations and Assessment

Our efforts to standardize will be focused on creating useful guidelines and assessment methods that assist businesses show they are following EU 5G security rules and give National Authorities standardized ways to evaluate compliance.

This means helping to create common security assessment criteria, compliance verification procedures, and reporting systems that help both businesses and regulators keep an eye on things in all EU Member States.

4.2.2 Target Standardization Bodies and Engagement Strategy

4.2.1.2 *The European Telecommunications Standards Institute (ETSI)*

ETSI is our main goal for contributions to technical standardization, especially through its Technical Committees on Cybersecurity (TC CYBER) and Mobile Standards Group (MSG).

Specific Areas of ETSI Involvement:

- The ETSI TS 103 645 series on cybersecurity for consumer Internet of Things devices is getting bigger to incorporate security standards for IoT devices that are connected to 5G.
- ETSI EN 303 645 cybersecurity standards, which add 5G-specific methods for assessing security
- ETSI TC CYBER working groups on protecting networks and information, giving feedback on how to protect 5G infrastructure
- ETSI NFV Security Group, which helps come up with ways to assess the security of virtualized 5G network functions

4.2.1.3 *The European Union's Cybersecurity Agency (ENISA)*

ENISA is an important partner for SAND5G standardization initiatives since it helps coordinate EU cybersecurity policy and helps Member States put cybersecurity measures into place.

ENISA's main goals for getting involved:

- 5G Security Standards and Guidelines: Helping ENISA with its ongoing work on 5G security by providing practical evaluation methods and implementation advice based on the capabilities of the SAND5G platform.
- Cybersecurity Certification Framework: Helping to create cybersecurity certification schemes under the Cybersecurity Act, especially for 5G infrastructure and services
- Threat Intelligence and Information Sharing: Helping ENISA with its work on cybersecurity information sharing frameworks by using automated threat intelligence tools that were built in SAND5G.
- Support from National Authorities: Sharing best practices and ways to evaluate that can help other National Authorities meet EU cybersecurity standards

4.2.1.4 *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)*

Our work on international standardization will focus on helping to improve ISO/IEC standards that are directly related to managing cybersecurity and telecommunications security. We want to make sure that SAND5G contributions are in line with global best practices while keeping Europe's lead in 5G security standards.

ISO/IEC Standards to Aim For:

- The ISO/IEC 27001/27002 series on managing information security, which adds security controls and assessment procedures that are particular to 5G
- The ISO/IEC 27035 series on managing information security incidents gives you automated incident response tools and playbook guidelines.
- ISO/IEC 30141 on Internet of Things standard architecture, which adds to the security requirements for IoT implementations that use 5G
- ISO/IEC 23053 gives advice on how to create a cybersecurity framework and helps with realistic evaluation methods for 5G environments.

5 Conclusions

The deliverable has managed to present thoroughly the progress of SAND5G project on Dissemination, Exploitation, Standardisation & Sustainability activities. The project is progressing nominally in this area, following the strategy that was defined in deliverable 5.1.

In particular the deliverable has a) presented in detail the dissemination activities through journals, conference publications, webinars & workshops and events & exhibitions, b) cited all the communication activities via the project's website, social media channels, newsletters, press releases and promotional materials, c) explained thoroughly the exploitation & sustainability activities that each partner has undertaken and d) listed the clustering and standardization activities as well as the clustering and standardization plans.

The consortium has strong confidence that by the end of the SAND5G project all the targets and KPIs that concern Dissemination, Exploitation, Standardisation & Sustainability will be achieved.