



SAND5G NEWSLETTER

Security Assessments for
Networks and D services in 5G



May 2026 Issue # 6

A message from Prof. Paris Kitsos

Dear SAND5G Community,

Over the past months, SAND5G has continued to strengthen its impact through a series of dissemination and stakeholder engagement activities supporting the project's mission of enhancing cybersecurity and resilience in 5G infrastructures.

The consortium actively participated in events such as Patras IQ, as well as webinars and workshops focused on emerging cybersecurity challenges, secure 5G deployment, and European policy developments.

We are also pleased to announce an upcoming webinar focusing on cybersecurity through the lens of EU policies and regulations, which will further promote dialogue and knowledge exchange among researchers, industry representatives, and policymakers.

These activities reflect the strong collaboration and commitment of all consortium partners as we continue advancing the project's objectives and maximizing the long-term impact of SAND5G outcomes for secure and trustworthy next-generation networks.

I would like to sincerely thank all partners and supporters for their continued dedication and contribution to the success of SAND5G.

Professor Paris Kitsos
SAND5G Assistant Project Coordinator



Upcoming Webinar: Cybersecurity through the lens of EU Policies & Regulations



π N E T
EMERGING NETWORKS & APPLICATIONS

SAVE THE DATE

Cybersecurity through the lens of EU Policies & Regulations

Join us on
June 3rd at 12:00
Online



*Save
The
Date*

On **June 3rd**, SAND5G consortium partner p-NET Emerging Networks & Verticals will be holding an online webinar at 12:00 exploring the rapidly evolving EU cybersecurity regulatory landscape and its impact on organizations across Europe!

The webinar will examine how emerging EU policies are creating both new opportunities and important obligations in areas such as digital trust, data protection, AI governance, and network security. Expert speakers will provide practical insights into key regulatory frameworks shaping Europe's cybersecurity ecosystem.

Topics will include the relationship between the EU Digital Identity Wallet and GDPR, the impact of the AI Act on organizations deploying AI systems, the role of the Cyber Security Act and Cyber Resilience Act in strengthening cyber resilience, and the evolution from the 5G Security Toolbox toward a broader vision of trusted connectivity.

The webinar is supported by the SAND5G, CONSENTIS, CURIUM, and CUSTODES EU projects, bringing together experts from across the European research and innovation community.

Stay tuned for registration details through SAND5G and p-NET's sites and social media!

Patras IQ 2026 “CRA & CSA: Mandatory Cybersecurity Requirements for Digital Products in the EU”



With the support of the [SAND5G](#), [CURIUM](#), and [CUSTODES](#) EU Projects, and through their ongoing efforts to promote cybersecurity awareness, knowledge sharing, and stakeholder engagement around secure digital infrastructures, [p-NET Emerging Networks & Verticals](#) successfully organized the session “CRA & CSA: Mandatory Cybersecurity Requirements for Digital Products in the EU – The Deadline Is Approaching” during Patras IQ 2026, bringing together experts, researchers, and industry professionals to discuss the evolving European cybersecurity regulatory landscape.

Hosted at the Conference and Cultural Centre of the University of Patras, the session focused on the implications of the new EU cybersecurity framework introduced by the Cyber Resilience Act and the Cybersecurity Act for products with digital elements.

Through an engaging discussion structured around the 4W+1H approach (Who, What, Where, When, How), participants explored the new compliance requirements affecting companies that develop, import, or distribute products with digital elements in the EU. The session also highlighted the role of Cyber Ranges as practical environments for simulation, testing, and training to support cybersecurity readiness and regulatory compliance.

The session featured contributions from Argyro Chatzopoulou (APIROPLUS Services), Dr. Konstantinos Lampropoulos (University of Patras and p-NET Emerging Networks & Verticals), and Kostas Poullos (Sphynx).

As the deadlines for new cybersecurity obligations approach, discussions like these are increasingly important in helping organizations - particularly SMEs - prepare for upcoming regulatory changes and strengthen the security of digital products across the European market.

Webinar: “5G Cybersecurity through the Lens of Business”



p-NET Emerging Networks & Verticals, in collaboration with the SAND5G Project Consortium, successfully organized the online webinar “5G Cybersecurity through the Lens of Business” on February 25th, 2026. As part of the “Through the Lens of...” webinar series, the event explored the business dimension of cybersecurity in 5G+ ecosystems, with a focus on practical and scalable cybersecurity solutions for European SMEs.

The webinar was coordinated by Athanassios Staveris-Polykalas (p-NET Emerging Networks & Verticals) and featured presentations by Ovidiu Mihaila (Bitdefender), Kostas Poullos (Sphynx), and Wissam Mallouli (Montimage, France), who shared insights on cybersecurity as a business enabler, regulatory challenges, and effective approaches for strengthening cyber resilience in 5G+ environments.

The event concluded with an interactive discussion on AI-driven cybersecurity, NIS2-related requirements for SMEs, and the evolving cybersecurity landscape for next-generation networks.

SAND5G & CURIUM Workshop on Risk Assessment & Incident Response



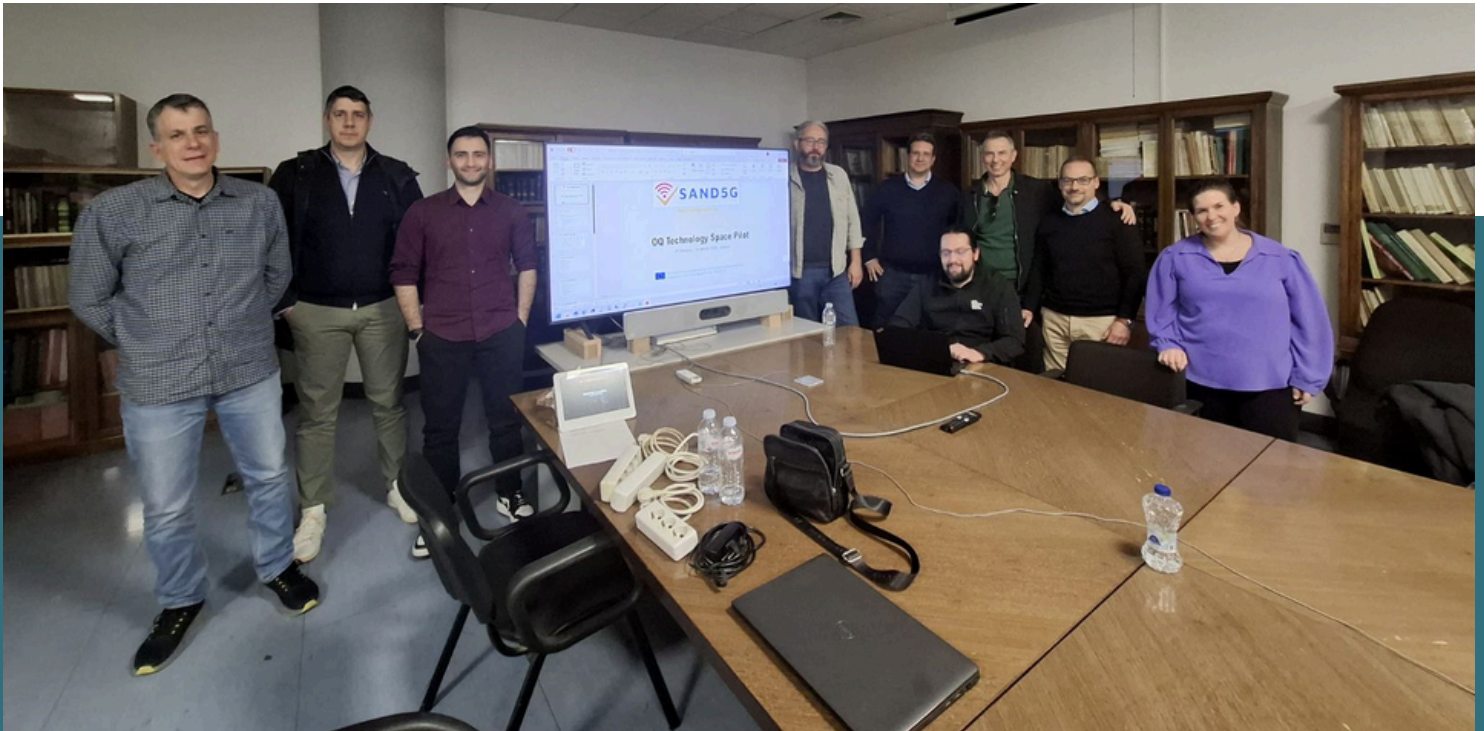
On February 13th, 2026, the SAND5G Project and the CURIUM Project jointly organized the interactive workshop “Risk Assessment & Incident Response,” bringing together participants for a hands-on exploration of key cybersecurity practices essential for today’s evolving digital landscape.

The workshop was led by Argyro Chatzopoulou and Apostolos Karras from APIROPLUS SOLUTIONS Ltd., who guided attendees through core concepts of risk assessment, incident response, and the practical implications of Murphy’s Law in cybersecurity operations.

The session focused on conducting practical risk assessments within organisations, preparing for and effectively managing cybersecurity incidents, and applying knowledge through hands-on exercises reflecting real-world challenges and solutions.

Through interactive discussions and practical examples, the workshop demonstrated how structured risk assessment and incident response practices enable organisations to navigate complex cybersecurity environments and support the secure deployment of next-generation 5G networks.

Strengthening Europe's 5G Resilience - Plenary Meeting



On March 13th, the SAND5G Project consortium held a plenary meeting in Athens, hosted by the National Cybersecurity Authority of Greece, partner of the SAND5G Consortium.

As 5G networks continue to become a critical part of Europe's digital economy, the meeting highlighted the importance of collaboration between technical innovators and national regulatory authorities.

Consortium partners focused on operationalizing the EU 5G Toolbox by aligning the project's risk-assessment platform with the strategic priorities and operational needs of national authorities.

Discussions also examined how the SAND5G solution can support regulatory oversight by helping authorities monitor and strengthen the security of critical infrastructures, while also exploring ways to align project outcomes with Greece's national cybersecurity strategy and broader digital ecosystem objectives.

Engage with us on social media and stay updated!



Our Consortium



The SAND5G project, "Security Assessments for Networks and services in 5G" 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.