



Resilmesh Final Event – online

Cyber Resilience in the AI Era

From European Research to Real-World Impact

Time: 10:00 - 12:10 CET Nov 11 2026

Please register for the event at:

https://tus-ie.zoom.us/webinar/register/WN_PNLAY8BBSomF5XL5G5Rpiw

Cybersecurity is entering a period of fundamental change.

Rapid advances in AI are changing what attackers can do, what defenders can automate, the speed at which both sides can operate, and ultimately how we need to think about cyber resilience. At the same time, critical infrastructure is becoming more interconnected across IT, OT, IIoT, cloud and edge environments.

Europe has invested significantly in cybersecurity research and innovation to address these challenges. Projects such as Resilmesh have generated technologies, operational experience and evidence across real critical-infrastructure environments.

The challenge now is not only what we can research or develop. It is how we turn European research into capabilities that are adopted, deployed and sustained in the real world.

The Resilmesh Final Event goes beyond presenting project results and uses the experience of Resilmesh as the starting point for a broader European conversation around two transformations happening simultaneously:

1. The AI transformation of cybersecurity itself. AI is changing attacks, defence, security operations and the technological capabilities available to organisations.

2. The transition from research to market and operational deployment. Europe needs stronger bridges between public institutions, Research and Technology Organisations (RTOs), universities, cybersecurity companies, investors and end users if publicly funded innovation is to become operational capability.

This event explores where these two transformations meet.

How can Europe turn the next generation of AI-enabled cybersecurity research into operational capabilities?

Agenda

10:00–10:05 — Welcome & Setting the Scene

Cyber Resilience at an Inflection Point

Speaker: Dr Brian Lee, Technological University of the Shannon, IE; Resilmesh Project Coordinator

10:05–10:20 — European Perspective

The New Cybersecurity Landscape: AI, Resilience and Europe's Strategic Priorities

Speaker: Mr. Konstantinos Kokosis, Programme Manager DG CNECT Unit for Cybersecurity and Innovation, Resilmesh Project Officer

10:20–11:10 — Resilmesh: From Research to Operational Evidence

What Did We Learn?

Resilmesh results are organised around three connected lessons that reflect the progression from understanding complex infrastructures, to anticipating threats, to supporting effective resilience:

CONTEXT-> INTELLIGENCE -> ACTION

1. Understanding What Matters: Assets, Services and Dependencies

Resilience in the AI era begins with understanding the system itself. As AI increasingly supports threat detection, prediction and decision-making, organisations need the operational context to understand what those insights actually mean. Resilmesh explores how this context can be built across interconnected IT, OT, IIoT, cloud and edge environments by identifying assets, services and the dependencies between them.

Speaker: Dr Martin Husak, Masaryk University, CZ

2. From Detection to Anticipation – What AI adds

AI can strengthen cyber resilience by helping organisations detect, analyse and anticipate threats more quickly and at greater scale. Building on the operational context provided by assets, services and dependencies, Resilmesh explores how AI-based anomaly detection, attack prediction, penetration testing and decision support can help security teams move beyond identifying that an incident has occurred towards understanding how a threat may evolve and where action may be needed next.

Speaker: Dr Branka Stojanovic, Joanneum Research, AT

3. From Risk to Resilience: Turning Insight into Action

Understanding risk and identifying threats only strengthen resilience when they lead to effective action. Resilmesh explores how situational awareness, asset and dependency context, threat intelligence and risk assessment can be brought together to support prioritisation, response and mitigation across critical-infrastructure environments.

Speaker: Dr Jorge Bernal Bernabe, University of Murcia, ES

4. The Real-World Test

Short presentation from pilots and Open Call participants focused on what Resilmesh enabled in real operational environments:

- What did you test in practice?
- How did Resilmesh support or enable what you were trying to achieve?
- What did you learn about the role and value of AI in that real-world environment?

The objective is to show how the capabilities discussed in the previous sessions translated into practice, what worked in real critical-infrastructure settings.

Speakers: Mr Jacopo Tamagnini; Mr Pedro Branco Xilbi Sistemas; Mr Esteban Vazquez Ferreiro , Tesla Technologies

11:10–12:00 — Main Panel

From Research to Deployment: Building Europe's Next Generation of Cybersecurity Capabilities.

- What does AI change for critical-infrastructure resilience?
- Why do strong European research results struggle to reach operational deployment
- What would a better European pathway from research to capability look like?

Participants:

- *Mr. Konstantinos Kokosis, DG CNECT*
- *Mr. Vjeran Piršić , Eko Kvarner*
- *Dr Sheikh Mahub Habib, Head of Product Cybersecurity and Privacy Innovation, AUMOVIO SE*
- *Dr. Vasileios Mavroeidis, Assistant Professor, University of Oslo*

Moderator: Dr Jassim Happa, Royal Holloway University

12:00-12:10— Closing

From Resilmesh to What's Next

The technological environment is moving extremely quickly. AI is changing the capabilities available to attackers and defenders alike. The next challenge for Europe is therefore not only to continue producing excellent cybersecurity research, but to become equally effective at turning research into technology, technology into products, and products into capabilities deployed across European organisations and critical infrastructure.

The final Resilmesh event can be a place to start that conversation!