Resilmesh

securing cyber infrastructures

Resilmesh Newsletter

June - August 2026

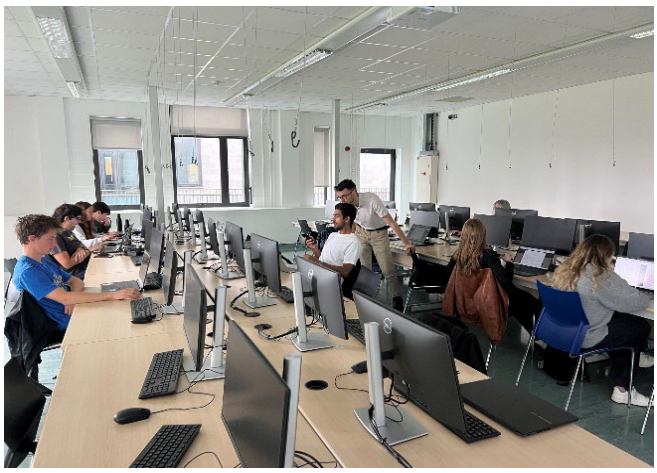
Resilmesh Summer School: Cyber Defence Essentials

Funded by the European Union

From 8-12 June 2026, the Resilmesh project, in collaboration with the RUN-EU University Network, hosted the week-long “Cyber Defence Essentials” Summer School at the Technological University of the Shannon (TUS). Throughout the week, participants gained a practical grounding in the key stages of the cyber defence process, based on the NIST Cybersecurity Framework, with particular emphasis on Protect, Detect, Respond and Recover.

Combining theory with hands-on learning, the programme also featured a two-day cyber range exercise hosted by Resilmesh partner JAMK University of Applied Sciences in Finland. Through a Capture the Flag (CTF) exercise, participants had the opportunity to apply their knowledge in a realistic cyber environment and work with tools developed within the Resilmesh project.

The Summer School offered participants an opportunity to strengthen their practical cybersecurity skills, while experiencing how Resilmesh technologies can support cyber defence and resilience in real-world scenarios.



Resilmesh Technical Webinar: Connected and Interoperable Cybersecurity Operations

On 24 June 2026, Resilmesh hosted the online technical webinar “Connected and Interoperable: A Mesh Approach to Dispersed and Edge Infrastructure Cybersecurity Operations.” The session explored the growing cybersecurity challenges of increasingly distributed digital infrastructures and presented how Resilmesh, an EU Horizon-funded initiative delivering a next-generation Security Operations and Analytics Platform Architecture (SOAPA) purpose-built for distributed and edge environments, is addressing these challenges.

The webinar focused on two key capabilities at the heart of the Resilmesh Collaboration Mesh: X-MESH, an open standards-based orchestration layer built on CACAO, OpenC2, and STIX/TAXII that enables intelligence to flow from detection through to enforcement across heterogeneous and dispersed deployments; and CHAMELEON, a NATS-native resilient service mesh designed to eliminate

single points of failure and maintain continuous, secure communications even under active attack or node failure.

Together, X-MESH and CHAMELEON demonstrated how connected and interoperable cyber operations can work in practice — coordinated at the control level, resilient at the communications level, and coherent across distributed infrastructures.

The full session is available on the Resilmesh YouTube channel.onnected

Resilmesh
securing cyber infrastructures

Resilmesh at SecSoft 2026 in Berlin

On 3 July 2026, Resilmesh was represented at the 8th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft 2026), co-hosted with the 12th IEEE International Conference on Network Softwarization (NetSoft 2026) in Berlin, Germany.

Representing the Resilmesh consortium, Michael Somma (JOANNEUM RESEARCH DIGITAL) presented the paper "Environment-Grounded Multi-Agent Workflow for Autonomous Penetration Testing," while Lukáš Sadlek (Masaryk University) presented "Intelligence Augmentation in a Platform for Cyber Situational Awareness." Both papers have been published in IEEE Xplore and are also available through the Resilmesh website.

In addition, Lukáš Sadlek participated in the workshop's poster session, presenting the Resilmesh project and providing participants with the opportunity to learn more about its objectives, technologies, and work towards strengthening cybersecurity and resilience in software-defined and virtualized infrastructures.

The participation provided an important opportunity to share Resilmesh research outcomes with the scientific and cybersecurity community and increase the project's visibility within the field.

Resilmesh
securing cyber infrastructures

Resilmesh at the 1st Webinar of the 2026 ECSCI Cluster Webinar Series

On 20 July 2026, Resilmesh participated in the 1st Webinar of the 2026 ECSCI Cluster Webinar Series, bringing together the Resilmesh, SONIC and MIRANDA projects to showcase the latest European research and innovation in cyber resilience, AI-driven cybersecurity and secure critical infrastructures.

Representing Resilmesh, Brian Lee from the Technological University of the Shannon (TUS) delivered the session "Cyber Situational Awareness for Dispersed Systems." The presentation highlighted RESILMESH's work on security orchestration and analytics, AI-driven threat detection and critical infrastructure pilots, demonstrating how the project is contributing to enhanced cyber situational awareness and resilience across dispersed environments.

The webinar also featured contributions from the SONIC and MIRANDA projects, addressing complementary topics including zero-trust architectures, threat intelligence sharing, distributed monitoring, anomaly detection and privacy-preserving telemetry. Interactive Q&A sessions provided participants with the opportunity to engage directly with the speakers and explore emerging approaches to securing resilient digital infrastructures.

The event provided an important platform for knowledge exchange and collaboration across European cybersecurity projects, while increasing the visibility of Resilmesh research and technological developments within the wider ECSCI community.

The recording of the webinar is available on the Resilmesh YouTube channel.

Stay Connected

Stay tuned to our social media channels for updates on their progress and upcoming Resilmesh initiatives.

Resilmesh

securing cyber infrastructures

Resilmesh

securing cyber infrastructures

Follow Resilmesh

Funded by the European Union