RESILMESH POLICY BRIEF

Resilmesh
securing cyber infrastructures

ADVANCING CYBER RESILIENCE AND OPERATIONAL PREPAREDNESS THROUGH CYBER RANGE EXERCISES

European and national cybersecurity preparedness frameworks[i,ii] provide an opportunity to strengthen the operational readiness of Critical Infrastructure (CI) organisations through recurring, evidence-driven Cyber Range (CR) exercises. Such exercises should combine realistic incident scenarios, common investigative datasets, accessible cybersecurity tools and structured workflows reflecting the responsibilities of Security Operations Centres (SOCs), Computer Security Incident Response Teams (CSIRTs) and CI security personnel. The Resilmesh[iii] experience demonstrates the practical application of this approach, with participants recognising the training's value for professional development and its relevance to real-life cybersecurity operations.

The Challenge: Turning Cybersecurity Capabilities into Operational Preparedness

Europe's critical digital infrastructures increasingly integrate legacy Information Technology (IT), Operational Technology (OT), connected devices, and cloud services, creating complex environments exposed to evolving cyber threats. Technology alone cannot ensure preparedness. Effective incident response requires practitioners to analyse heterogeneous security information, correlate evidence, reconstruct incidents and make informed decisions under uncertainty. Traditional awareness activities and isolated technical exercises are not adequately reflecting these operational demands. The challenge is to translate cybersecurity knowledge and technological capabilities into demonstrable operational readiness through realistic, repeatable and systematically evaluated exercises that strengthen individual competencies and organisational response capabilities.

Resilmesh Findings

The Resilmesh project addressed these preparedness challenges through two investigation-based CR exercises involving realistic cybersecurity scenarios. The findings highlight three principles that can inform the design and adoption of future cybersecurity preparedness exercises.

Realism matters. CR exercises should reflect the operational environments and responsibilities of cybersecurity practitioners. In both Resilmesh exercises, 85.71% of respondents positively assessed the relevance of the exercise content to real-life situations, highlighting the value of scenarios grounded in practical cybersecurity challenges.

Investigation matters. Effective incident response depends on analytical reasoning rather than familiarity with individual tools alone. The Resilmesh approach engaged participants in examining security evidence, correlating information from multiple sources and reconstructing incidents through structured investigative workflows representative of SOC and CSIRT operations.

Consistency and evaluation matter. Common, publicly available investigative datasets and controlled exercise conditions can support reproducibility and meaningful comparison of learning outcomes. Combined with systematic evaluation, this approach enables CR exercises to generate evidence of competency development and inform continuous improvements in cybersecurity preparedness.

Policy Direction: Towards a Common European Approach to Evidence-Driven Cyber Range Exercises

Building on the Resilmesh findings, European and national cybersecurity authorities should promote a common methodological approach to CR exercises as instruments for strengthening CI preparedness and operational resilience. This approach should establish shared principles for exercise design, delivery and evaluation, while allowing adaptation to sector-specific threats, operational environments and organisational needs. Particular emphasis should be placed on realistic incident scenarios, reproducible investigative conditions, accessible cybersecurity tools and measurable learning outcomes.

Recommendations for action

Integrate recurring Cyber Range exercises into CI preparedness programmes. National competent authorities should encourage CI operators to incorporate realistic, investigation-based exercises into their cybersecurity preparedness and resilience programmes. Moving beyond occasional training activities, recurring exercises would enable organisations to strengthen operational competencies, identify capability gaps and monitor progress over time.

Establish common principles for exercise design and delivery. European and national cybersecurity actors should develop methodological guidance defining the

Funded by
the European Union

essential characteristics of effective CR exercises. Drawing on Resilmesh results, they should include realistic incident scenarios, common or controlled investigative datasets, structured workflows and clearly defined objectives. A shared methodological baseline would promote consistency and comparability while preserving flexibility across CI sectors and organisations.

Align exercise scenarios with operational responsibilities. CR exercises should reproduce the investigative activities performed by SOCs, CSIRTs and CI security personnel. Tasks should involve interpreting security alerts, analysing and correlating evidence, validating indicators of compromise, reconstructing incidents and supporting operational decision-making.

Promote reproducible and accessible exercise environments. European and national initiatives should encourage the use of interoperable, preferably open-source cybersecurity tools and reusable investigative datasets. This would facilitate the replication and adaptation of exercises across organisations, reduce dependence on specific proprietary solutions and support wider access to practical cybersecurity training.

Introduce systematic, evidence-based evaluation of exercise outcomes. CR exercises should incorporate predefined learning objectives and assessment criteria that capture investigative performance and competency development. Evaluation should extend beyond participation and satisfaction indicators to examine how effectively practitioners analyse evidence, reconstruct incidents and apply investigative procedures. The resulting evidence should provide feedback to support continuous improvement in exercise design and organisational preparedness programmes.

Pathways towards European Cyber Resilience

Resilmesh focus group discussions and debriefing sessions provided additional insights into the wider adoption and sustainability of evidence-driven cybersecurity preparedness. These qualitative insights inform four complementary pathways through which European and national cybersecurity actors could strengthen the accessibility, consistency and long-term contribution of CR exercises to CI resilience.

Establish European repositories of reusable cybersecurity exercise resources. European and national cybersecurity actors should explore the development of trusted repositories containing sector-specific incident scenarios, reusable investigative datasets, exercise templates and supporting training materials.

These repositories would facilitate knowledge transfer, reduce duplication of effortsectors and support the adaptation of exercises across different CI sectors.

Develop maturity frameworks for organisational cyber-exercise capabilities. A structured maturity framework could help CI organisations assess and progressively improve their ability to prepare for, conduct and evaluate cybersecurity exercises. Maturity levels should reflect increasing operational complexity, ranging from introductory technical exercises to integrated investigations, multi-team coordination and organisation-wide incident response. Such frameworks could support capability planning and continuous improvement.

Translate European Cybersecurity Preparedness Requirements into Measurable Operational Capabilities. European and national authorities should explore how structured CR exercises and their evaluation results can contribute to the preparedness objectives established under the NIS2 Directive[i] and the EU Cyber Solidarity Act[ii]. Common exercise methodologies and documented outcomes would support organisational preparedness assessments and inform national cybersecurity strategies, while respecting the distinct legal requirements and responsibilities established by these instruments.

Promote cross-sector and cross-border cybersecurity exercises. European initiatives should encourage collaborative exercises involving CI operators, SOCs, CSIRTs and relevant public authorities from different CI sectors and Member States. Building on common investigative methodologies, these exercises would provide opportunities to practise information sharing, coordinated investigation and incident response across organisational and national boundaries, contributing to collective European cyber resilience.

[i] ***Directive*** (EU) 2022/2555 *https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng*

[ii] ***Regulation*** (EU) 2025/38 *https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng*

[iii] ***Resilmesh*** EU-funded project: *https://resilmesh.eu/* and *https://cordis.europa.eu/project/id/101119681*

Funded by the European Union