
Funded by
the European Union

1 Executive Summary

This White Paper presents the evidence and lessons learned from *two investigation-based Cyber Range exercises conducted within the Resilmesh EU-funded project*. Unlike conventional competition-oriented exercises, the Resilmesh approach placed investigation at the centre of capacity building. Participants analysed pre-generated datasets derived from realistic smart-grid attack scenarios and followed structured workflows representative of those employed by SOCs and CSIRTs. The exercises integrated professional cybersecurity tools for monitoring, threat intelligence, forensic analysis, structured investigation, and collaboration, creating a realistic yet controlled learning environment with consistent investigative conditions within each exercise.

Across the two exercises*, one hundred and seventy (170) members of the cybersecurity community registered, sixty-two (62) successfully completed the full training programme and forty-two (42) provided evaluation feedback*. The exercises also reached substantially different populations: Exercise 1 was mainly practitioner-oriented (*57.14% cybersecurity practitioners*), while Exercise 2 was predominantly learner-oriented (*50.0% cybersecurity learners*). In both exercises, 85.71% of evaluation respondents positively rated the relevance of the training content to real-life situations *positively,* while their feedback indicated improvements in practical cybersecurity investigation skills.

The findings demonstrate the potential of Cyber Ranges to evolve beyond technical training environments into strategic instruments for developing and assessing operational cyber resilience.

Five principal lessons emerged. *(1) Cyber resilience is built through investigation rather than memorisation; (2) realistic operational workflows provide greater learning value than isolated technical exercises; (3) integrated tool ecosystems strengthen situational awareness; (4) structured preparation improves exercise effectiveness; and (5) continuous evaluation is essential for sustainable capacity building***.** Together, these findings demonstrate that **effective cyber resilience requires the integration of skilled practitioners, realistic scenarios, interoperable technologies, structured investigative methodologies, and evidence-driven continuous improvement**.

The White Paper therefore recommends that:

1. Critical Infrastructure operators integrate regular investigation-based CR exercises into organisational resilience programmes
2. Public authorities support cross-sector and cross-border Cyber Range infrastructures and common evaluation methodologies
3. Training providers adopt realistic, competency-based capability development approaches and systematically evaluate learning outcomes
4. Technology developers prioritise interoperability and analyst-centred investigation workflows.

Looking ahead, AI-assisted investigations, Large Language Models, Digital Twins, threat-informed exercises, federated Cyber Ranges, and cross-border IT/OT scenarios can further

transform Cyber Ranges into strategic instruments for strengthening Europe's collective cyber resilience.

2 The Challenge

2.1 From Awareness to Operational Readiness

The cybersecurity landscape protecting critical infrastructures (CI) has evolved significantly over the last decade. Digitalisation, increasing interconnectivity between Information Technology (IT) and Operational Technology (OT), widespread adoption of cloud services, and increasingly sophisticated adversaries have transformed the nature of cyber incidents. Modern attacks are rarely isolated technical events; they increasingly exploit weaknesses across people, processes, and technologies. Consequently, cybersecurity professionals require more than awareness of threats or theoretical knowledge of defensive technologies. They must be able to analyse large volumes of heterogeneous security data, correlate evidence across multiple sources, validate indicators of compromise (IoCs), reconstruct attacker activity, and make informed operational decisions when information is incomplete or uncertain. These capabilities are difficult to develop through classroom instruction alone. They require practical experience in realistic environments where practitioners can repeatedly investigate representative incidents without placing operational systems at risk.

The experience gained through Resilmesh supports a broader proposition: Cyber Ranges should evolve from technical training environments into evidence-driven instruments for developing and assessing operational cyber resilience.

2.2 Why Traditional Cyber Exercises Often Fall Short

Cybersecurity exercises are a central component of workforce development, and their design strongly influences the capabilities they aim to develop. Many conventional exercises emphasise offensive techniques, competitive scoring, rapid vulnerability exploitation, or the completion of predefined technical tasks. These approaches can be highly effective for developing specific technical skills, but they do not necessarily reproduce the analytical processes that characterise operational incident response.

Within Security Operations Centres (SOCs), Computer Security Incident Response Teams (CSIRTs), and CI security operations, investigations rarely begin with complete information or follow a predetermined path. Analysts must identify relevant evidence among large volumes of telemetry, distinguish legitimate from malicious activity, formulate and test hypotheses, correlate information across different systems, and progressively reconstruct an incident.

Exercise design also presents an evaluation challenge. Dynamically generated attacks may vary according to infrastructure conditions, network performance, attacker behaviour, and participant interaction. Participants can therefore encounter different evidence or attack progressions, making objective comparison of learning outcomes difficult.

Future cyber exercises should consequently balance operational realism with sufficiently consistent exercise conditions, enabling practitioners to experience realistic investigative complexity while supporting systematic evaluation of learning outcomes.

2.3 Why Operators Need Practical Investigation Skills

CI operators increasingly depend on SOC analysts, CSIRT personnel, incident responders, and security specialists to detect, investigate, and contain cyber incidents before they disrupt essential services. Their effectiveness depends not only on technical knowledge or familiarity with individual security tools, but on their ability to transform fragmented technical information into operational understanding.

During real incidents, practitioners must work with incomplete and evolving information, determine which evidence is relevant, connect observations across multiple sources, and make informed decisions under uncertainty. These capabilities require a combination of **technical expertise, investigative reasoning, and situational awareness** that is difficult to develop through theoretical instruction or isolated technical exercises alone.

Capacity-building programmes should therefore provide opportunities to practise **end-to-end cyber investigation under realistic conditions**, connecting technical knowledge with the analytical and decision-making processes required during operational incident response.

2.4 Why Cyber Ranges Matter

Cyber Ranges (CRs) provide a controlled environment in which these capabilities can be developed without exposing operational infrastructure to risk. They enable realistic cyber incidents to be recreated within isolated environments where practitioners can investigate, experiment, make decisions, and learn from their actions. Their value, however, extends beyond technical simulation. A mature CR can bring together realistic scenarios, operational datasets, cybersecurity tools, communication mechanisms, structured learning activities, and evaluation processes within a common environment. This makes it possible to connect technical training with operational workflows and organisational preparedness.

The **Realistic Global Cyber Environment (RGCE)** is the Cyber Range infrastructure of **Jamk University of Applied Sciences** that hosted the two RESILMESH exercises. The RGCE supports a six-stage capability development process.

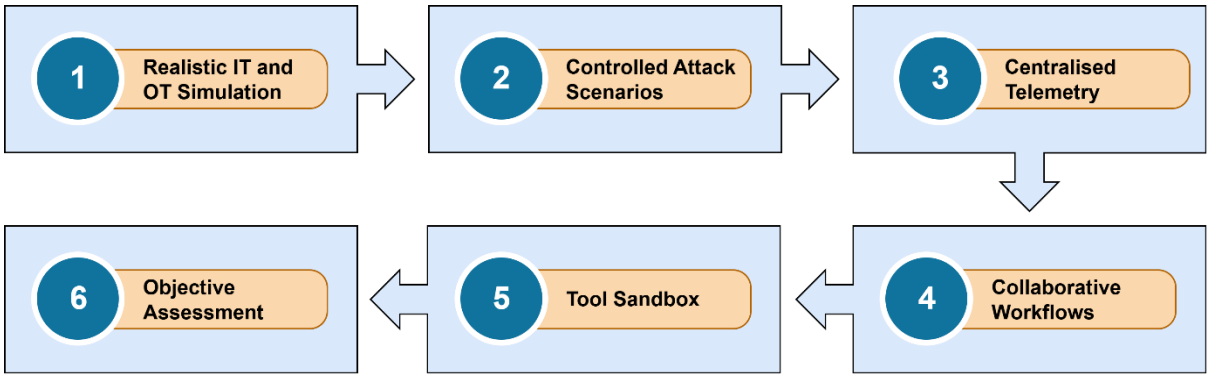

Figure 1. 6-stage Cyber Range Capability Lifecycle

For CI organisations, CRs can therefore serve simultaneously as environments for **skills development, operational rehearsal, methodology validation, and capability assessment**.

2.5 Towards Evidence-Based Capacity Building

Effective cybersecurity capacity building should not be evaluated solely through participation numbers, completion rates, or participant satisfaction. Organisations also need evidence

about whether training strengthens relevant operational competencies, whether scenarios accurately reproduce investigative challenges, and where technical, methodological, or organisational improvements are required.

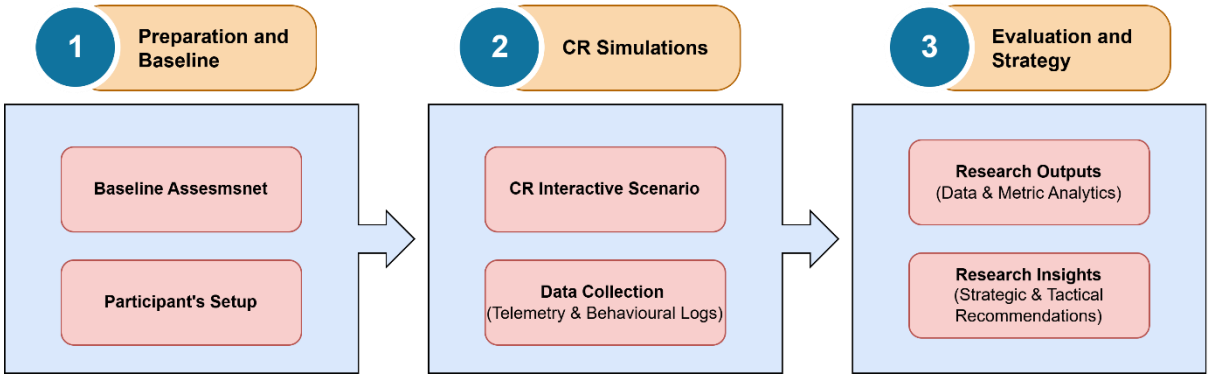

Figure 2. Resilmesh Cyber Range Research Design and Evaluation Methodology

The Resilmesh exercises were consequently conceived not merely as training events but as a structured research and evaluation process. The methodology combines three interconnected stages: **Preparation and Baseline, Cyber Range Simulations, and Evaluation and Strategy**. Baseline information establishes participants' initial knowledge and experience; CR simulations provide practical investigation experience; and operational observations, platform data, questionnaires, predefined KPIs, and participant feedback provide quantitative and qualitative evidence for evaluation.

This evidence-based cycle allows each exercise to inform the next iteration of training, scenario design, technology integration, and capacity-building strategy. In this sense, evaluation becomes an integral component of operational readiness rather than simply a post-exercise activity.

3 The Resilmesh Approach

3.1 Building Operational Cyber Resilience through Investigation-Based Capacity Building

Resilmesh translated the need for operationally focused capacity building into an investigation-based CR methodology combining realistic scenarios, structured investigative workflows, professional cybersecurity tools, controlled datasets, and evidence-based evaluation.

> *The methodology was implemented through two online Cyber Range exercises, each conducted in a distinct environment with its own scenario and combination of cyber-defence tools. Despite these differences, both followed the same underlying principle: participants progressed through a structured investigation rather than a collection of isolated technical challenges.*

The methodology therefore served two complementary purposes: **to provide participants with practical experience of operational cyber investigation** and **to generate evidence for assessing and improving the training approach, exercise design, and supporting technologies**.

3.2 Investigation Rather Than Competition

A defining characteristic of the Resilmesh methodology was its emphasis on **systematic investigation rather than competitive performance**. Participants were not rewarded for being the fastest to detect a vulnerability or complete an isolated technical task. Instead, they progressed through a common incident narrative and a structured sequence of investigative activities reflecting operational incident-response practice.

Within each exercise, all participants analysed the same security events and forensic artefacts, ensuring consistent conditions for participants undertaking that specific exercise. This common baseline enabled the exercises to focus on analytical reasoning, evidence correlation, hypothesis development, and decision-making, while supporting meaningful comparison of participant experiences and learning outcomes within each exercise.

3.3 A Structured Learning Journey

Participants first received preparatory material, including an Online Open Course introducing the smart-grid environment, the Resilmesh platform, and the tools used during the exercises. Registration, onboarding, account provisioning, and technical validation ensured that participants could focus on investigation rather than technical setup.

The exercises were conducted within the fully isolated Realistic Global Cyber Environment, the Cyber Range operated by Yamk University of Applied Sciences. Within this environment, participants investigated representative attack scenarios using realistic operational workflows. Throughout the exercises, participants received guidance through structured analytical challenges while maintaining sufficient freedom to develop their own investigative strategies.

Following completion, learning outcomes were evaluated through questionnaires, operational metrics, participant feedback, and exercise observations. The results were subsequently analysed to identify technical improvements, methodological refinements, and recommendations for future exercises, creating a continuous improvement cycle that strengthens both the training methodology and the supporting platform.

3.4 Learning Through Operational Workflows

The technical environment was designed to reproduce the sequence of activities commonly performed during operational cyber investigations.

Across the two exercises, participants used different combinations of cyber-defence and investigative tools according to the respective scenario and environment. Security alerts generated through **Wazuh** provided initial indications of suspicious activity, which could be enriched with threat intelligence available through **MISP**. Detailed forensic analysis, evidence correlation, and timeline reconstruction were then performed using various investigative tools, including the **Elastic Stack**, which was used extensively in the first exercise. **CTFd** was used to structure the analytical challenges and capture participant progression, while **Rocket.Chat** supported communication and technical assistance throughout the exercises.

The purpose of this integrated toolchain was not to train participants in individual products in isolation. Instead, it required them to move between different information sources, validate findings, and correlate evidence across platforms. The resulting workflow reproduced an

essential characteristic of operational incident response: situational awareness emerges through the synthesis of heterogeneous evidence rather than from a single security tool.

3.5 Realistic Scenarios, Repeatable Evidence

The two exercises addressed different smart-grid cybersecurity scenarios. Exercise 1 focused on **unauthorised device activity and ransomware affecting IT/OT environments**, while Exercise 2 addressed **a multi-stage investigation involving IT and OT elements.** Although the scenarios differed in their context and investigative pathway, both exposed participants to realistic security artefacts and required them to identify, analyse and correlate evidence throughout the investigation.

Rather than dynamically executing attacks during each participant session, **Resilmesh used pre-generated and validated datasets** reproducing the evidence generated by the respective scenarios. Within each exercise, participants therefore investigated a common body of incident evidence under consistent conditions. **This reduced variability associated with live attack execution and infrastructure performance while preserving the analytical complexity of incident investigation. It also enabled organisers to reproduce the respective scenarios, compare participant experiences within each exercise, and systematically refine the training methodology**.

3.6 Developing Operational Competencies

The Resilmesh methodology was designed around a set of operational competencies relevant to cybersecurity investigation and incident response. These competencies were organised into **five interconnected areas**:

i. **Detection and Interpretation:** Recognising and interpreting indications of suspicious or potentially malicious activity;

ii. **Threat Hunting and IoC Validation:** Investigating beyond initial alerts and assessing indicators against available evidence and threat intelligence;

iii. **Evidence Correlation**: Connecting information from heterogeneous sources and analytical platforms;

iv. **Incident Reconstruction**: Establishing relationships between events to develop a coherent understanding of attacker activity;

v. **Analytical Reasoning and Decision-Making**: Assessing incomplete evidence, testing assumptions, and developing evidence-based conclusions.

These competencies shift the emphasis from proficiency with individual tools to the ability to **transform fragmented technical evidence into operational understanding**.

3.7 Measuring Learning and Continuous Improvement

Evaluation was embedded throughout the exercise lifecycle. Operational exercise metrics, platform statistics, participant engagement data, structured questionnaires, learning-outcome assessments, predefined project KPIs, and qualitative feedback were combined to assess both participant experience and the effectiveness of the methodology.

Evaluation activities were conducted by Resilmesh partners who were not involved in operating the CR, providing additional separation between exercise delivery and evaluation.

The resulting evidence was used to identify improvements in challenge design, platform usability, participant preparation, exercise delivery, and evaluation methodology.

Each exercise therefore functioned simultaneously as a **capacity-building activity and an evidence-generation mechanism**, allowing lessons from one iteration to inform subsequent training and methodological development.

3.8 The Resilmesh Capacity Building Framework

The two exercises demonstrate a capacity-building model based on the integration of five mutually reinforcing elements:

Figure 3. Investigation-first Cyber Range methodology

The Resilmesh model therefore treats the CR simultaneously as a training environment, an operational investigation environment, and an evidence-generation mechanism. It provides the controlled environment connecting realistic incidents with practitioner behaviour, professional tools, measurable learning activities, and systematic evaluation. The Resilmesh approach therefore provides a practical foundation for moving Cyber Ranges beyond isolated technical training events towards **strategic instruments for developing, assessing, and continuously improving operational cyber resilience**.

4 Who Participated

The two Resilmesh exercises engaged a diverse cybersecurity community comprising learners, practitioners, educators, and researchers. Participants ranged from learners developing their cybersecurity competencies to experienced SOC analysts, incident responders, cybersecurity specialists, researchers, educators, and other technical professionals. Recruitment was conducted through Resilmesh partners, professional and academic networks, international cybersecurity events, European research communities, and targeted outreach to cybersecurity and critical-infrastructure communities.

The two cybersecurity exercises conducted within the Realistic Global Cyber Environment (RGCE) attracted a total of **170 registrations**. Exercise 1, conducted in November 2025, attracted **51 prospective participants**, of whom **17 actively participated** in the exercise and **14 completed the evaluation**. Exercise 2, conducted in June 2026, attracted **119 registrations**, with **45 active participants** and **28 evaluation responses**. In total, the evaluation therefore captured feedback from **42 participants** across the two exercises.

Furthermore, the participant profiles differed between the exercises. Exercise 1 was predominantly practitioner-oriented, while Exercise 2 attracted a larger proportion of learners. This variation provided insight into how investigation-oriented CR training is experienced by participants with different professional and educational backgrounds and should be considered when interpreting and comparing the evaluation results.

5 Investigation-Based Learning

Investigation-based learning places the **reasoning process** at the centre of cybersecurity training. Rather than learning individual technologies or completing predefined tasks in isolation, participants are confronted with an evolving incident in which relevant information must be identified, interpreted, and progressively transformed into an understanding of what occurred.

This approach reflects an important distinction between **technical knowledge and operational competence**. Knowing how a cybersecurity tool functions does not necessarily mean that a practitioner can determine when to use it, recognise which information is relevant, relate its output to evidence obtained elsewhere, or translate technical observations into an informed assessment of an incident.

In an investigation-based model, the learning therefore occurs through the decisions participants make as the investigation develops. They must determine what to examine, assess the significance of available evidence, challenge assumptions, and revise their interpretation as new information emerges. The emphasis shifts from finding a predefined answer towards developing a **structured and evidence-based reasoning process**.

The CR provides a suitable environment for this form of learning because realistic investigative complexity can be reproduced without exposing operational infrastructure to risk. Within each Resilmesh exercise, participants worked with a common body of incident evidence, providing consistent conditions in which different investigative approaches and learning experiences could be observed and evaluated.

Investigation-based learning consequently provides a bridge between **cybersecurity education and operational practice**. It connects technical knowledge with the analytical judgement required to investigate real incidents and provides the learning mechanism through which the operational competencies defined in the Resilmesh methodology can be practised.

6 Operational Competencies in Practice

The two Resilmesh exercises provided a practical, functional environment in which the targeted operational competencies could be applied as part of a coherent investigation. Rather than being exercised independently, the competencies were connected through the progression of the incident, requiring participants to move from initial indications of suspicious activity towards an evidence-based understanding of what had occurred.

This progression reflects the interdependent nature of operational cyber investigation. **Detection** and **interpretation** initiate the investigative process. **Threat hunting** and **IoC validation** extend the analysis beyond initial observations. **Evidence correlation** establishes relationships across information sources, while **incident reconstruction** brings these findings together into a coherent account of attacker activity. Throughout this process, **analytical reasoning and decision-making** guide how evidence is assessed and conclusions are formed.

The five competency areas therefore represent an interconnected investigation workflow rather than independent technical skills.

Figure 4. Investigation workflow applied in the Resilmesh Cyber Range exercises

7 Measuring Capacity Building Effectiveness

Evaluation of the two Resilmesh exercises combined operational metrics, participant engagement data, structured questionnaires, qualitative feedback, and predefined KPIs. This enabled a structured assessment of both the exercises and the overall capacity-building methodology. Across the two exercises, 170 registrations were recorded, 62 participants actively engaged in the exercises, and 42 provided evaluation feedback. Registrations increased from 51 in Exercise 1 to 119 in Exercise 2, demonstrating the considerably greater reach achieved by the second training activity.

7.1 Real-World Relevance and Professional Applicability

Participant feedback demonstrated a strong perceived connection between the exercises and real-world cybersecurity practice. **85.71% of respondents positively rated the relevance of the training content to real-life situations.** This indicates that the investigation-based scenarios and workflows were broadly perceived as representative of practical cybersecurity challenges.

Professional applicability differed between the exercises. **85.71% of Exercise 1 respondents and 60.71% of Exercise 2 respondents** recognised the applicability of the acquired knowledge to their professional responsibilities. This difference should be interpreted alongside the different participant profiles, particularly the larger proportion of learners participating in Exercise 2.

7.2 Practical Skills and Learning Value

Participant feedback indicated improvement in practical cybersecurity investigation skills and demonstrated the perceived learning value of applying operational competencies within realistic incident scenarios. Rather than assessing proficiency with individual tools, the exercises provided participants with opportunities to practise integrated investigative reasoning representative of SOC and CSIRT activities.

The evaluation also generated evidence for improving the training itself. Participant feedback and exercise observations identified areas for refinement in challenge design, platform usability, participant preparation, exercise delivery, and evaluation methodology, allowing lessons from each exercise to inform subsequent capacity-building activities.

7.3 From Evaluation to Evidence-Based Capacity Building

The results demonstrate the value of combining quantitative indicators with qualitative participant feedback and exercise observations. The evidence does not merely describe participation or satisfaction; it provides a basis for assessing the **relevance, applicability, and**

perceived learning value of investigation-based Cyber Range training while identifying areas for continuous improvement.

This evidence provides the foundation for the **five core findings** presented in the following section.

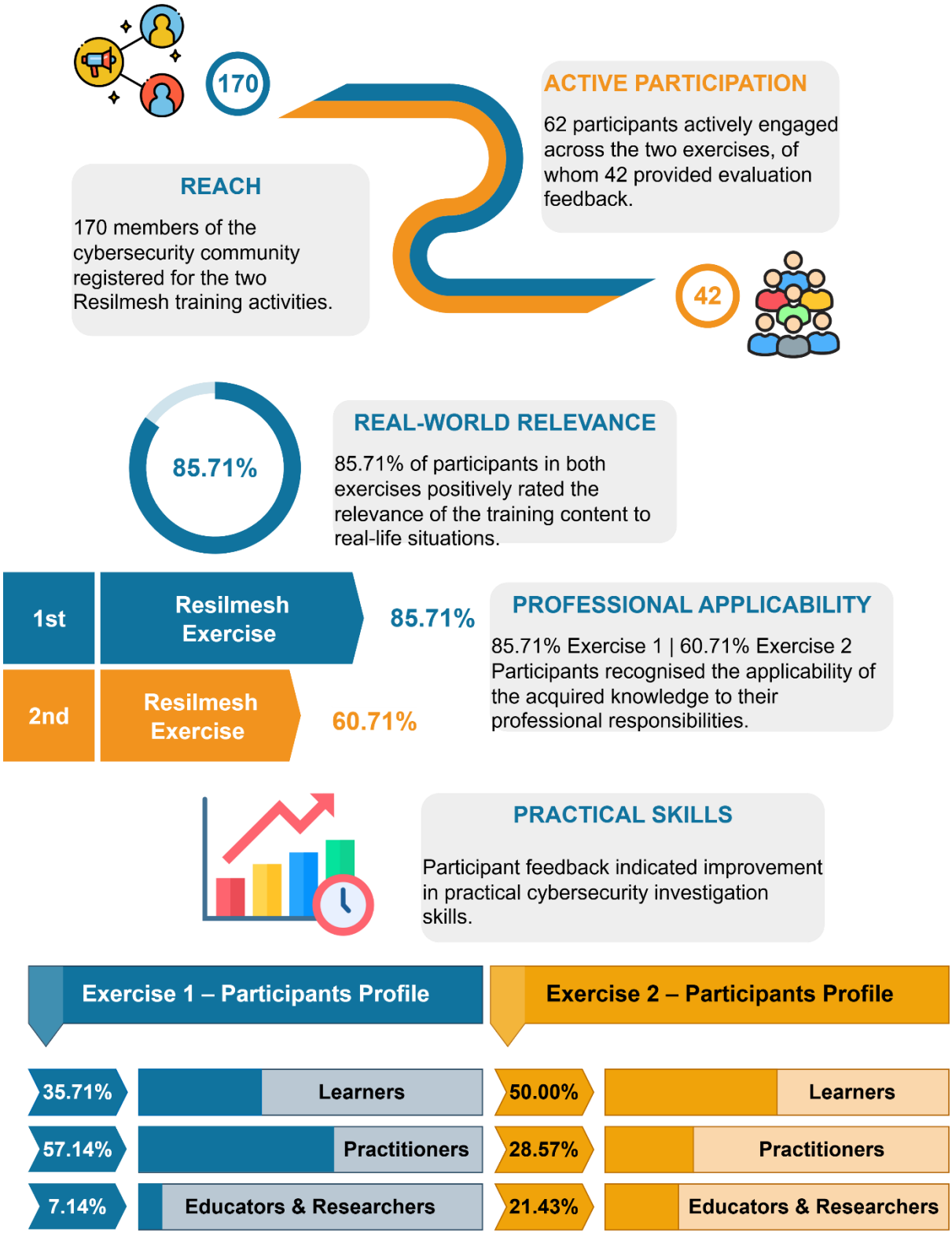

Figure 5. Resilmesh Training Evidence at a Glance

8 Core findings

The Resilmesh exercises generated practical evidence on how investigation-based CR training can support the development of operational cybersecurity competencies. Analysis of participant behaviour, exercise observations, learning outcomes, and post-exercise evaluations consistently highlighted five principles that should guide the design of future cyber resilience programmes. Although derived from smart grid scenarios, these lessons are equally relevant to other CI sectors, including ***energy***, ***transport***, ***water***, ***healthcare***, ***telecommunications***, and ***public administration***.

8.1 Lesson 1: Cyber Resilience is Built Through Investigation, Not Memorisation

Operational incident response requires more than technical knowledge. Analysts must interpret incomplete evidence, correlate information, test hypotheses, and adapt their understanding as an investigation evolves. Resilmesh therefore shifted the emphasis from predefined technical tasks towards **structured investigation**, requiring participants to analyse realistic attack artefacts and develop evidence-based conclusions. The experience indicates that **CR training should develop analytical reasoning alongside technical proficiency**.

8.2 Lesson 2: Realistic Operational Workflows Strengthen Training Relevance

Real incidents require analysts to move across detection, threat intelligence, forensic analysis, and incident-response activities. The Resilmesh exercises reflected this through scenario-driven investigative workflows, progressing from initial detection and validation to evidence correlation and incident reconstruction. This approach connected individual technical tasks to the broader investigation and reinforced the **importance of operational realism in CR design**.

8.3 Lesson 3: Integrated Tool Ecosystems Support Situational Awareness

Effective cyber investigation depends on correlating information from multiple sources rather than relying on individual security tools. Across the Resilmesh exercises, participants used different combinations of monitoring, threat-intelligence, forensic, and collaboration tools to investigate incidents and validate findings. The experience highlighted the importance of **interoperability and integrated investigative workflows** in supporting situational awareness and analyst decision-making.

8.4 Lesson 4: Preparation Enables Effective Exercise Participation

Effective CR training begins before the exercise itself. Resilmesh combined participant onboarding, technical validation, and preparatory material to familiarise participants with the operational context and exercise environment. This preparation helped establish a common baseline and allowed participants to focus more effectively on **investigation, evidence correlation, and decision-making** during the exercises.

8.5 Lesson 5: Continuous Evaluation is Essential for Sustainable Capacity Building

Cyber exercises should generate evidence for improving both participant capabilities and future training activities. Resilmesh combined participant feedback, engagement data, observations, and predefined KPIs to assess the exercises and identify areas for improvement. Evaluation should therefore be treated not simply as the final stage of an exercise, but as an input into the **next cycle of scenario design, training, and capability development**.

These five lessons illustrate that effective cyber resilience depends on far more than technical proficiency. ***Investigation-based learning***, ***realistic operational workflows***, ***integrated analytical environments***, ***structured preparation***, and ***evidence-driven continuous improvement*** form the foundation of sustainable cyber capacity building. They provide a practical basis for translating the Resilmesh experience into approaches applicable across CI sectors.

9 Recommendations

The findings and lessons derived from the Resilmesh exercises translate into four recommendations for the principal stakeholder groups involved in cybersecurity capacity building. These recommendations provide practical directions for translating investigation-based CR training into sustainable organisational and European cyber resilience practices.

9.1 Strengthening Organisational Preparedness

Regular participation in CR exercises should become an integral component of organisational resilience programmes rather than an isolated training activity. Investigation-based exercises allow practitioners to develop and maintain operational competencies under realistic conditions while exposing capability gaps that may not be apparent through conventional training. Capacity building should therefore be treated as a continuous process that evolves alongside emerging threats, technologies, and organisational needs.

Critical Infrastructure operators should integrate regular investigation-based Cyber Range exercises into organisational resilience programmes.

9.2 Supporting a European Cyber Resilience Ecosystem

Public authorities can strengthen collective cyber resilience by supporting accessible CR infrastructures and organising exercises that reflect the interdependencies of European CIs. Cross-sector and cross-border exercises can facilitate knowledge exchange and expose participants to incidents extending beyond organisational boundaries. Common evaluation methodologies and indicators would further support consistent assessment of exercise outcomes and evidence-based approaches to cybersecurity capacity building.

Public authorities should support cross-sector and cross-border Cyber Range infrastructures and common evaluation methodologies.

9.3 Advancing Cybersecurity Education and Training

Cybersecurity training should progressively move beyond knowledge acquisition towards the development of measurable operational competencies. Realistic scenarios, structured investigative workflows, and systematic evaluation can provide participants with opportunities to practise analytical reasoning, evidence correlation, and decision-making. Training should also incorporate adequate preparation and familiarisation with the exercise environment, enabling participants to focus on investigation rather than technical or procedural barriers**.** Evaluation should assess not only participant experience but also the extent to which exercises contribute to practical capability development and operational readiness.

Training providers adopt realistic, competency-based capability development approaches and systematically evaluate learning outcomes.

9.4 Designing Technologies that Support Investigation

Cybersecurity technologies should support coherent investigative processes rather than operate as isolated components. Interoperability between monitoring, threat-intelligence, forensic-analysis, and incident-management platforms can facilitate evidence correlation, improve situational awareness, and support analyst decision-making. Technology design should therefore consider not only individual technical capabilities but also how effectively tools integrate into operational investigative workflows.

Technology developers should prioritise interoperability and analyst-centred investigation workflows.

10 Looking Ahead

Cyber threats targeting CI continue to evolve rapidly, driven by increasing digitalisation, greater interconnectivity between IT and OT environments, and the emergence of increasingly sophisticated attack techniques. Consequently, **CR training approaches must evolve** accordingly. While these technologies and approaches were not evaluated through the two Resilmesh exercises, the investigation-based methodology provides a foundation that could be extended to emerging CR capabilities.

Future cyber resilience programmes are expected to incorporate AI to support investigation and decision-making, including Large Language Models (LLMs) that assist analysts during incident investigation, automate documentation, and facilitate knowledge sharing. Digital Twins (DTs) of critical infrastructures will enable highly realistic simulation of operational environments, allowing practitioners to investigate complex attacks while accurately modelling the behaviour of physical systems. The growing maturity of autonomous SOCs will further transform training by introducing intelligent assistants capable of supporting analysts while preserving human oversight in critical decisions.

Cyber exercises should also become increasingly threat-informed and continuously updated using current threat intelligence and adversary tactics to maintain operational relevance. Rather than being organised as isolated annual events, CRs should support continuous training programmes that enable practitioners to progressively strengthen their competencies throughout their professional careers.

Finally, the future of European cyber resilience lies in collaboration. Federated CRs capable of connecting multiple organisations and countries will facilitate large-scale cross-border exercises that reflect the interconnected nature of European CIs. Such environments will enable the simulation of hybrid IT/OT attacks, cascading incidents across sectors, and complex interdependencies between energy, transport, telecommunications, healthcare, and other essential services. These capabilities will provide decision-makers and practitioners with a far more comprehensive understanding of systemic cyber risks while strengthening Europe's collective resilience against future threats.

Editors

George Kokkinis, KEMEA – Center for Security Studies,

Tuomo Sipola, JAMK University of Applied Sciences, Institute of Information Technology

Genny Dimitrakopoulou, KEMEA – Center for Security Studies

Acknowledgements

The research leading to this White Paper was funded by the European Union under the Resilmesh project (Grant Agreement No. 101119681). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

References

- Resilmesh Consortium. (2026). *D6.4 – Capacity building exercise report*. Available at: https://cordis.europa.eu/project/id/101119681/results. Interim version available at: https://resilmesh.eu/deliverables/
- Kokkinis, G., Kapsalis, N., & Dimitrakopoulou, G. (2026). Resilmesh investigation-based Cyber Range exercises evaluation (Version 1.0) [Dataset]. Zenodo. https://doi.org/10.5281/zenodo.22673203
- Saarelma, M., Sipola, T., Taari, N., & Ålander, N. (2026). RESILMESH-JAMK-SG-Exercise1-Attacks [Data set]. Jamk University of Applied Sciences. https://doi.org/10.23729/fd-e16800f0-ece2-36e5-b122-28bbbf9b78f0