NITRO | Newsletter

Issue 3| May 2025

Connected 5G-IoT Cyber Range for Training and Secure Operation

Project Coordinator

Prof. Christos Xenakis

School of Information and Communication Technologies
Department of Digital Systems,
University of Piraeus,
Karaoli and Dimitriou 80,
PC 18534, Piraeus, Greece

Tel: +30 210 4142776

Email: xenakis@ssl-unipi.gr

Project Details

G.A. number: 101145872

Project Website: nitro-project.eu

Project start: 01/01/2024

Duration: 36 Months

Total cost: EUR 1862656

EC Contribution: 101145872

The NITRO consortium is now preparing to submit key deliverables that comprehensively document the project's progress to date. In parallel, significant advancements have been made in defining the full suite of cybersecurity training exercises to be integrated into the final cyber range platform.

The upcoming deliverables will also outline the core components of the project's gamification strategy, including mechanisms for trainee accreditation, marking a major milestone in the development of NITRO's scoring and feedback systems.

Looking ahead, the consortium is intensifying efforts in WP3 (Cyber Security Training Exercises) and WP4 (Scoring System and Gamification), while also advancing preliminary integration planning and finalising the overall architecture.

CONSORTIUM

NITRO project has received funding from the European Union's DIGITAL JU SME Support Actions under the grant agreement No. 101145872.

Emerging Cyber Threats in 5G Networks

The evolution of 5G introduces a transformative communications infrastructure. However, this same evolution also opens new vectors for sophisticated cyber threats. With its distributed architecture, increased virtualisation, and critical role in digital ecosystems, 5G requires an adaptive security posture.

Threat	Description	Implications
Virtualisation Exploits	Exploitation of virtualised network functions and slices via misconfigurations or hypervisor vulnerabilities.	Unauthorised access, service disruption, cross-slice attacks.
Supply Chain Attacks	Compromise of hardware or software components introduced during manufacturing or update cycles.	Persistent backdoors, data leakage, systemic infrastructure compromise.
AI-Powered Attacks	Use of AI for automated reconnaissance, vulnerability discovery, and adaptive exploitation techniques.	Faster and stealthier breaches, particularly against ML-based defence systems.
Side-Channel & Timing Attacks	Leveraging timing information or hardware emissions to extract sensitive data from edge devices or base stations.	Exposure of credentials, cryptographic material, and user metadata.
Network Slicing Abuse	Misuse of logical network partitions to gain unauthorised privileges or isolate attacks from detection systems.	Data exfiltration, slice hijacking, degradation of service quality for targeted users or applications.

The increasing attack surface of 5G calls for a paradigm shift in threat modeling and security engineering. Proactive threat intelligence, AI-driven anomaly detection, and strong inter-slice isolation mechanisms will be key to defending the next-generation network infrastructure.

NITRO project has received funding from the European Union's DIGITAL JU SME Support Actions under the grant agreement No. 101145872.

Building Robust AI for 5G Security

As artificial intelligence becomes integral to securing 5G networks, ensuring its own robustness is essential. AI systems deployed for threat detection, traffic analysis, and anomaly identification must be designed to withstand adversarial manipulation, model evasion, and data poisoning.

Key Approaches for Enhancing AI Robustness in 5G Security

- Adversarial Training
  Involves training AI models using crafted malicious inputs to improve resilience against evasion and poisoning attacks.

- Ensemble Learning
  Leverages multiple models working in parallel to improve decision reliability and reduce vulnerability to targeted failures.

- Defensive Distillation
  A technique that transforms the model's sensitivity to input variations, making it more robust to subtle adversarial perturbations.

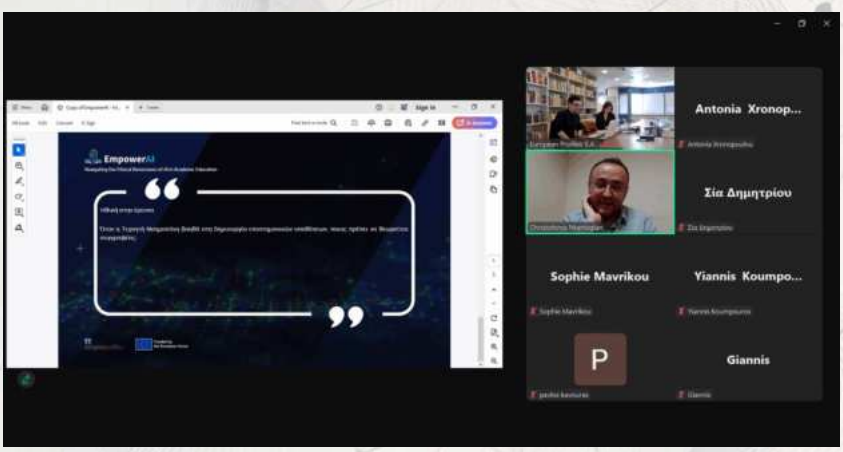
- Regularisation Techniques (Dropout & Noise Injection)
  Introduces randomness during model training to enhance generalisation and prevent overfitting, which is critical in dynamic 5G environments.

- Transfer Learning
  Applies pre-trained, security-hardened models to 5G contexts, reducing development time and increasing baseline robustness.

AI is not only a key enabler of 5G security but also a potential attack vector. Embedding resilience into AI pipelines is vital to maintaining trust and functionality across mission-critical 5G systems.

NITRO project has received funding from the European Union's DIGITAL JU SME Support Actions under the grant agreement No. 101145872.

NITRO News & Events



NITRO Project Advances Secure AI Education Through European Collaboration

Addressing the Cybersecurity Skills Gap at the 12th Information Security Conference

NITRO project has received funding from the European Union's DIGITAL JU SME Support Actions under the grant agreement No. 101145872.

NITRO Project Presented at Infocom Security 2025 in Athens

ARES Calls for participation

Ghent, Belgium, August 11-14, 2025

NITRO Co-Organizes the 5th International Workshop on Advances on Privacy Preserving Technologies and Solutions. (IWAPS 2025)

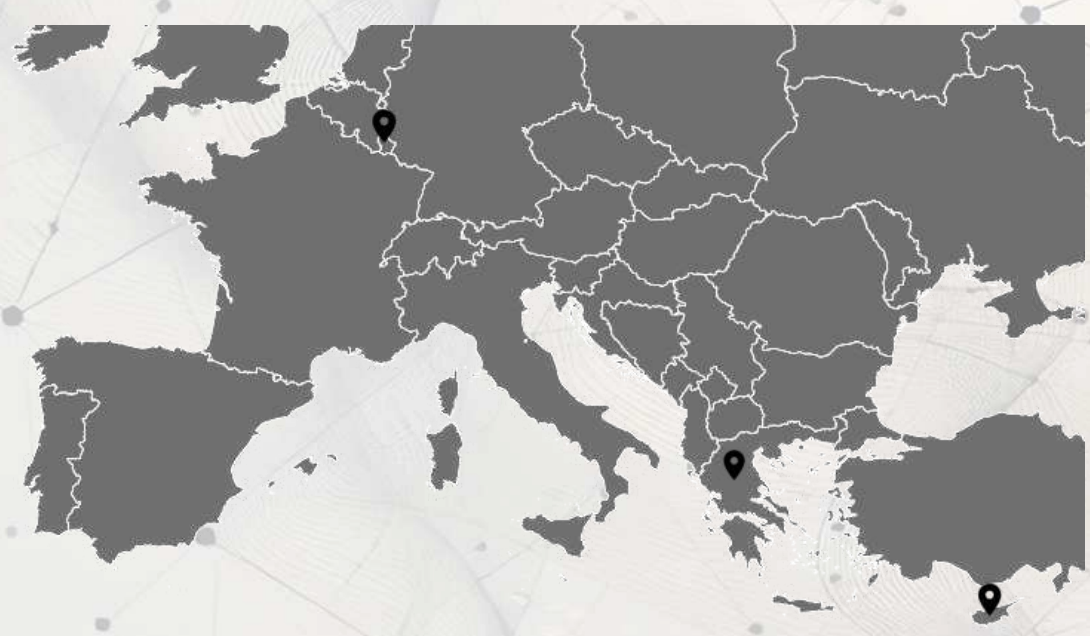
NITRO project has received funding from the European Union's DIGITAL JU SME Support Actions under the grant agreement No. 101145872.

Upcoming Deliverables and Future Activities

NITRO researchers are working on deliverables and tasks in order to fulfill all the main objectives which will lead toward the completion of the project.

In the next months, researchers will work *on the following deliverables*:

- D1.3: Project management report—first version
- D3.1: NITRO security training exercises design and development—first version
- D4.1: NITRO scoring and gamification system—first version
- D6.2: NITRO dissemination, communication and exploitation activity—second version



Find us here!

Website: nitro-project.eu

@nitroEUDEA

NITRO project has received funding from the European Union's DIGITAL JU SME Support Actions under the grant agreement No. 101145872.