AI IN DEFENCE SUMMIT 2026

BRUSSELS
2nd FEBRUARY 2026

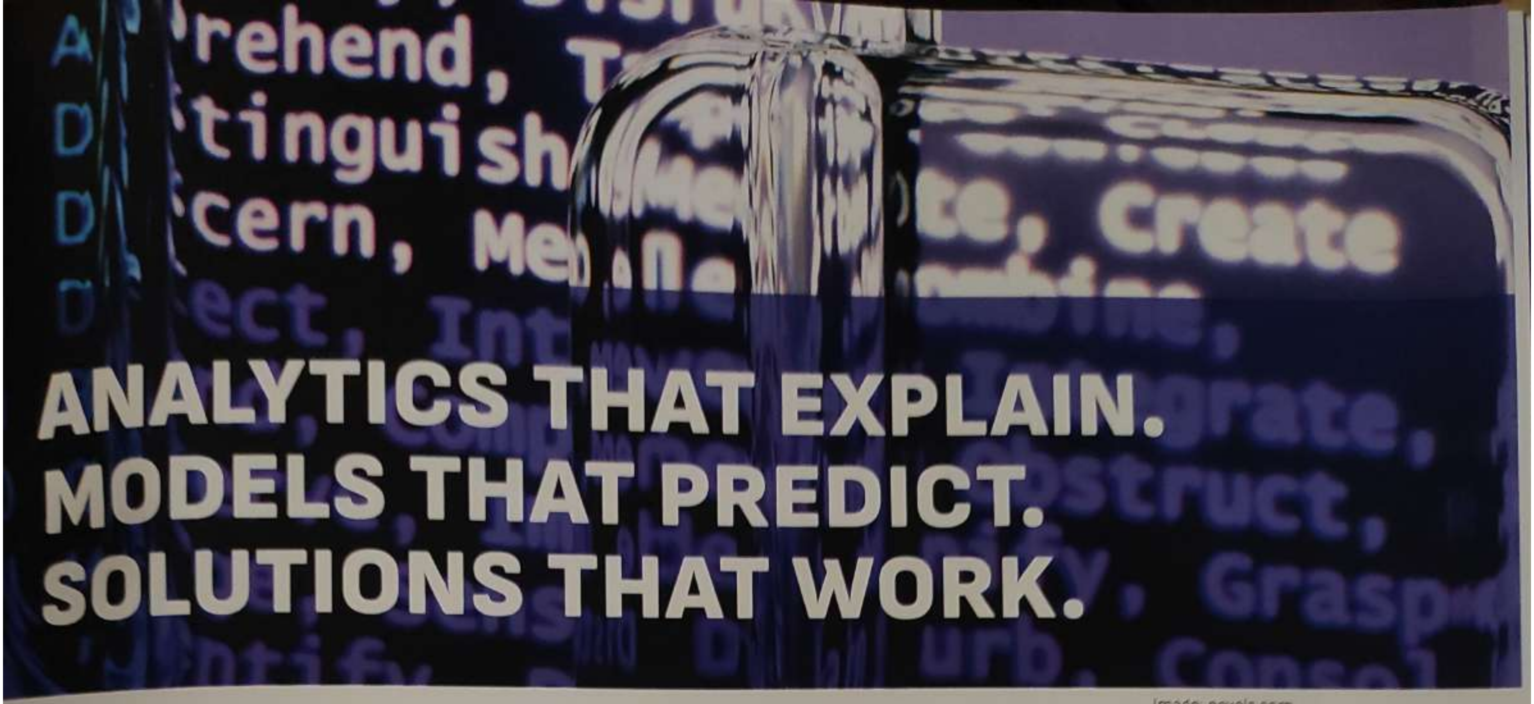
SECURING EUROPE'S CRITICAL INFRASTRUCTURE

COUNTERING RUSSIA'S HYBRID WARFARE

DEFENSE AI: AUTONOMY OR DELAY

THE CORRIDOR FOR DEFENSE STARTUPS

SEVENCAPITAL



ANALYTICS THAT EXPLAIN. MODELS THAT PREDICT. SOLUTIONS THAT WORK.

Image: pexels.com

The current realities of Russia's aggression against Ukraine are fostering fundamental shifts in how modern warfare is perceived by Western democracies, EU members, and NATO. Western policymakers and defence officials have officially acknowledged that the line between peace and war has been permanently blurred; cyberattacks, sabotage, and disinformation are now viewed as direct preparations for military confrontation.

The experience Ukraine has gained in countering hybrid influence is no less significant than its experience in battlefield victories and containment. The Institute for National Resilience and Security brings together specialists and scholars who have worked on projects countering Russian hybrid influence since 2014. By combining expertise in the humanities with mathematical sciences, we have created a unique environment for implementing innovative developments into state decision-support systems.

This synergy allows the Institute to act comprehensively — working simultaneously with technologies and meanings, with data and with people. This interdisciplinarity establishes the Institute as an intellectual hub for cooperation between the state, the academic community, business, media, and civil society.

The Institute's primary goal is to build an ecosystem of researchers, analysts, and practitioners in international and national security, specifically to mitigate the consequences of hybrid threats from the Russian Federation and its geopolitical allies.

In December 2025, the forum "Resilient Europe: Countering Russian Propaganda and Disinformation" gathered over 100 participants from 20 countries. During the event, Rena Marutian, Director of the Institute for National Resilience and Security, presented the Institute's first analytical product: the study "Strategic Resilience amid Hybrid Influence: Expert Recommendations and Strategic Implications Overview." By analysing the information landscapes of France, Spain, and Belgium, the study identified destructive narratives and the organisations systemati-

Ellina Shnurko-Tabakova

Institute for National Resilience and Security and the AI Lab

Institute for
National Resilience
and Security

Entity and Relationship Extraction

Using RAG (Retrieval-Augmented Generation) technologies, we extract entities from massive text datasets to build relationship graphs. Proprietary monitoring solutions, such as Attack Index, are integrated to enhance accuracy.

Institute for National Resilience and Security

Methodological Advantages. The Lab relies on four complementary approaches:

1. Semantic Networking: creating causal networks as explanatory models of reality.

2. "Swarm of Virtual Experts": applying identical prompts across various LLMs from different roles and positions, followed by statistical generalisation.

3. RAG Technologies: integrating LLMs with proprietary search and analytical systems to reduce hallucinations and increase topicality.

4. No-Code Prompt Programming: automatically transforming simple queries into structured prompts using logical primitives and formalised reasoning schemes.

Dmytro Lande

Institute for National Resilience and Security and the AI Lab

> ”
> The Institute, its Analytical Centre, and the AI Lab are ready for cooperation with state authorities, international organisations, and the private sector, offering solutions that turn complexity into structure and data into informed decisions.

Modern Large Language Models (LLMs) have opened a new era of automated analytics, yet they possess fundamental flaws critical to governance and security — such as hallucinations, "laziness," the "black box" effect, and outdated knowledge. The Lab systematically overcomes these limitations by combining LLMs with formalised knowledge and proprietary frameworks.

Our goal is to build a manageable, explainable, and responsible intellectual environment. The Institute, its Analytical Centre, and the AI Lab are ready for cooperation with state authorities, international organisations, and the private sector, offering solutions that turn complexity into structure and data into informed decisions.

Rena Marutian

Institute for National Resilience and Security and the AI Lab cally disseminating them, providing a foundation for professional dialogue with European partners.

For the AI in Defence Summit, the Institute has prepared a special edition of this research, featuring additional data on Russia's nuclear blackmail, technological myths, and further forecasts. This study is a joint product of the Institute's Analytical Centre and the AI Lab.

The Artificial Intelligence Laboratory is the core of the Institute's technical wing. It focuses on deploying AI solutions within the security and defence sectors: big data analysis, information threat monitoring, scenario modelling, and management decision support. Here, innovation is not an end in itself, but a tool to strengthen institutional capacity and resilience.

> ” The Lab unites experts with years of scientific and practical experience in AI, semantic analysis, information security, law, social communications, and scenario forecasting language.

Key Projects and Competencies.

Interactive Semantic Networks

We develop networks that map the structure of subject areas and the logic of interconnections between concepts, events, actors, and processes. These serve as the basis for analytical reports on complex security, social, and economic issues.

Causal Semantic Networks and Scenario Analysis. Using proprietary algorithms for bidirectional search (from cause to effect and vice versa), we:

▷ Model alternative scenarios.

▷ Identify critical points of influence.

▷ Rank scenarios by optimality criteria.

▷ Support decision-making in public policy and corporate governance.

Legal and Regulatory Analytics

The Lab performs a comprehensive analysis of legal texts using structured LLM prompts based on our proprietary no-code prompt programming framework. This identifies signs of lobbying, internal inconsistencies, corruption risks, and hidden shifts in norms.

Detection of Fakes and Manipulations

We counter disinformation by analysing the validity of connections within semantic networks, moving beyond surface-level fact-checking to the structural analysis of semantic distortions.

Targeted Communications

Based on expert-corrected semantic networks, we re-engineer content to generate texts for specific user categories, ensuring semantic integrity and relevance.