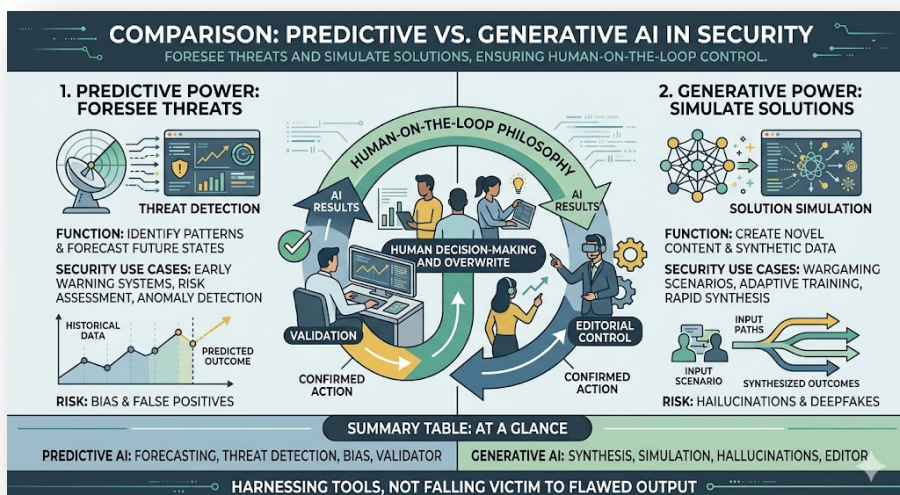


# Distinguishing Generative and Predictive AI

*AI is a force multiplier, not a replacement for command intent. By clearly distinguishing between the predictive power to foresee threats and the generative power to simulate solutions, while maintaining a rigorous "human-on-the-loop" philosophy, the security community can harness these tools without falling victim to their inherent flaws.*

By Dr. Gustavo Scotti di Uccio – AOS PDG<sup>1</sup>



**Descriptive:** analyzes data to understand what has happened (e.g., reports, dashboards, historical analysis).

**Diagnostic:** goes beyond description and seeks to explain why something happened.

**Prescriptive:** recommends actions based on data and predictions (e.g., decision-support systems).

**Reactive:** those that respond to real-time inputs without memory or continuous learning (e.g., some AI in games).

**Limited-memory,** uses past data to improve decision-making (e.g., many modern machine learning applications).

**Symbolic:** Based on explicit rules (logic, expert systems)

**Machine Learning-based:** learns from data

**Narrow:** Designed for specific tasks (most AI systems today)

**General: Artificial General Intelligence:** Still theoretical, capable of performing any human cognitive task

In essence, “generative” and “predictive” describe what AI does, whereas other classifications explain how it works and how advanced it is.

In today’s operational environment, AI is often used as a catch-all label, masking a far more complex reality. “Artificial Intelligence” is not a single, unified capability but a spectrum of approaches that can be classified in multiple ways, by function, level of autonomy, or technical architecture. While the distinction between generative and predictive AI is particularly useful, it represents only one lens among many.

The distinction between generative AI and predictive AI is useful, but it is only one of many ways to classify artificial intelligence. In fact, there is no single, universally accepted set of “categories,” since classification depends on the criteria used (function, capability, technical approach, and so on).

That said, beyond generative and predictive AI, several other important categories can be identified:

<sup>1</sup> AOS is an Independent company registered in Belgium since 2012. It delivers technical, engineering, operational and management support for defence and security sector at national, European & transatlantic levels. In systems engineering & programme management for the development of complex & innovative projects. In last 5 years, AOS has carried out more than 80 NATO studies and EU projects in interoperability, emerging technologies, air defence, energy management, UAVs, & dual-use solutions. AOS team consists of senior managers & engineers from Belgium, the Cz. Rep., France, Germany, Italy, Luxembourg, Portugal & Spain with extensive experience in defence industries, Ministries of Defence, and EU institutions

However, for defence and intelligence professionals, understanding the structural divide between **Predictive AI** and **Generative AI** is no longer a technical luxury, it is a strategic imperative. While both paradigms rely on vast datasets, their objectives, operational logic, and failure modes are fundamentally different.

## Objectives and Differences

To employ these tools effectively, command structures must distinguish between the "Oracle" and the "Architect."

### Predictive AI: The Analytical Oracle

Predictive AI is designed to **identify patterns and forecast future states** based on historical data. It functions through statistical inference, determining the probability of a specific outcome. In a security context, it answers the question: *"Based on the past, what is likely to happen next?"*

- **Operational Goal:** Risk assessment, anomaly detection, and pre-emptive logistics.
- **Core Mechanism:** Mathematical models like regression, decision trees, and neural networks tuned for classification.
- **Defense Application:** Early warning systems, cyber-intrusion detection, and predictive maintenance.

### Generative AI: The Synthetic Architect

Generative AI aims to **create novel content**, text, images, synthetic data, or code, that mimics the distribution of its training data. Rather than predicting a single point of failure, it creates entire scenarios. It answers the question: *"Can you construct a plausible representation of X?"*

- **Operational Goal:** Content synthesis, automated reporting, and creative simulation.
- **Core Mechanism:** Large Language Models (LLMs) and Diffusion Models capable of high-dimensional creation.
- **Defense Application:** Wargaming scenario generation, automated malware polymorphism for testing, and rapid intelligence synthesis.

## Case Studies: Successes and Tactical Failures

### The Positive Horizon: Enhanced Capabilities

- **Predictive Success (Signal Intelligence):** In maritime security, predictive models analyse AIS (Automatic Identification System) data to identify "dark vessels." By recognizing subtle deviations from standard commercial shipping routes, the AI can alert Coast Guards to potential smuggling or illegal fishing before the vessel reaches territorial waters.
- **Generative Success (Adaptive Simulation):** Modern pilot training utilizes generative AI to create dynamic, non-scripted "aggressor" pilots in virtual dogfights. Unlike traditional AI that follows fixed loops, generative agents can synthesize new tactics on the fly, forcing trainees to adapt to unpredictable human-like manoeuvres.

### The Negative Edge: Risks of Misalignment

- **Predictive Failure (The Feedback Loop):** A predictive policing tool used in urban security once created a "circular logic" trap. By sending patrols to areas where historical arrests were high (often due to over-policing rather than higher crime), the AI predicted more crime in those areas, leading to further arrests and biased data. This resulted in a total loss of community trust and resource mismanagement.
- **Generative Failure (The Hallucination Crisis):** During a rapid intelligence briefing, a generative model was tasked with summarizing intercepted communications. The model "hallucinated" the mention of a specific biological agent that was never in the source text, nearly triggering a high-level biosecurity alert. This highlights the danger of LLMs prioritizing "fluency" over "factuality."

## Mitigating Algorithmic Risk

To prevent technical advantages from becoming operational liabilities, the following protocols are recommended:

### Verification of Data Provenance

Predictive AI is only as objective as its training set. Security agencies must audit datasets for **historical bias** and **adversarial poisoning** (where an enemy injects data to "blind" the algorithm). For Generative AI, organizations must deploy "Digital Forensics" to tag and track synthetic outputs to prevent them from being reabsorbed as "real" intelligence.

## The "Human-in-the-loop" Mandate

In the defence sector, the "Black Box" approach is unacceptable.

- **Predictive:** AI should provide a "Confidence Score" for every prediction.
- **Generative:** Human analysts must perform "Fact-Checking Passes" on every AI-generated report.

No kinetic or high-stakes strategic decision should ever be fully automated.

## Adversarial Red Teaming

Security models must be subjected to constant "Stress Testing." This involves attempting to trick the predictive model using **Adversarial Machine Learning** (e.g., subtle camouflage that renders a tank invisible to AI sensors) or "jailbreaking" generative models to extract sensitive training data.

## Implementation of Explainable AI (XAI)

The next generation of defence AI must be **explainable**. If a predictive model flags a specific flight as a "high-threat kamikaze drone," it must be able to highlight the specific variables (speed, heat signature, trajectory) that led to that conclusion. Transparency is the bedrock of trust between the commander and the machine.

**Summary Table: At a Glance**

Feature	Predictive AI	Generative AI
<b>Primary Function</b>	Forecasting & Classification	Synthesis & Creation
<b>Security Use Case</b>	Threat Detection / Logistics	Simulation / Briefing / Coding
<b>Primary Risk</b>	Bias & False Positives	Hallucinations & Deepfakes
<b>Human Role</b>	Validator of Probabilities 	Editor of Content 

