ASSESSED
INTELLIGENCE

ASSESSED SIGNAL

February 2026

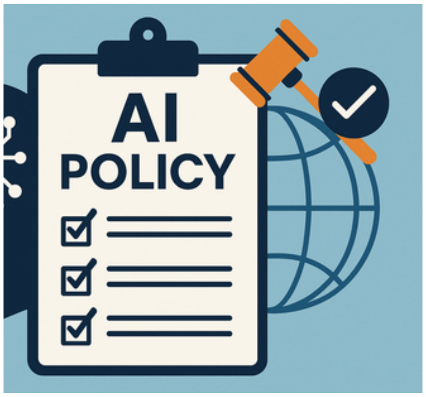
Intersection of Policy, Use Case, & Threat Intelligence

As AI becomes the focal point of more discussions in both government and industry, industry continues to adopt it for all the right reasons but fails to understand the risks and vulnerabilities such adoption entails. Anthropic doubles down on last month's report regarding the agentic AI attack. POTUS signs an executive order wresting federal control of AI regulation from the states to the executive branch.

Secure
&
Responsible
Technology.

AssessedIntelligence.com

The New Risk Framework



AI solves many problems. Some see it as the panacea. Companies are cinching budgets around its promise. However, AI creates new and sometimes unpredictable attack surfaces, and vulnerabilities. In this month's Signal, Assessed Intelligence will examine some of these issues in the face of Assessed's ARISE framework. The last part will delve into relative comparisons between the now 12 year old Diamond Threat Model, and the ARISE framework. The conclusion is that both work very well together, even though each has its own strengths and weaknesses.

https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/#:~:text=FOR%20ARTIFICIAL%20INTELLIGENCE-,Executive%20Orders,to%20United%20States%20AI%20leadership.

Disrupting AI Espionage

"...The next wave of innovation, agentic AI, operates as autonomous or semi-autonomous agents that can run code, interact with APIs, access databases, and make decisions on the fly. Organizations need to take immediate measures against security threats that can occur when software systems transition from producing passive text output to performing active operational tasks."

Agentic AI removes the intermediary, the operator from the next steps in a process, a query, or even a solution. Agents can trigger next steps, invoke new workflows, interact with databases that may contain sensitive information. Malicious actors can deceive agents into performing interactions that expose sensitive data. Feeding Retrieval Augmented Generation (RAG) systems with bad, incomplete or simply false information can trigger dangerous and unpredictable outcomes. Protocols like MCP, designed to help agents gain context, can be initially misconfigured for ease of use, leading to unexpected vulnerabilities.

The ARISE framework is very well-suited for AI related cyber intelligence because:

- AI threats are fast-moving and uncertain
- Evidence is often incomplete or indirect
- Policy decisions must be made before full certainty exists
- Agentic AI introduces emergent behavior that demands assumption-driven analysis

ARISE structures assessed intelligence by making assumptions explicit, reasoning transparent, indicators actionable, sources evaluated, and judments confidence-weighted—turning uncertainty into decision support.

https://www.anthropic.com/news/disrupting-AI-espionage

The UK is Exposed to Serious Threats from AI, an MP Warns

Consumers and the UK financial system are being exposed to "serious harm" by the failure of government and the Bank of England to get a grip on the risks posed by artificial intelligence, an influential parliamentary committee has warned. In a new report, MPs on the Treasury committee criticize ministers and City regulators, including the Financial Conduct Authority (FCA), for taking a "wait-and-see" approach to AI use across the financial sector. To date, the UK has not developed

Consumers and the UK financial system are being exposed to “serious harm” by the failure of government and the Bank of England to get a grip on the risks posed by artificial intelligence, an influential parliamentary committee has warned. In a new report, MPs on the Treasury committee criticize ministers and City regulators, including the Financial Conduct Authority (FCA), for taking a “wait-and-see” approach to AI use across the financial sector. To date, the UK has not developed any specific laws or regulations to govern their use of AI, with the FCA and Bank of England claiming general rules are sufficient to ensure positive outcomes for consumers. The report flagged a lack of transparency around how AI could influence financial decisions, potentially affecting vulnerable consumers’ access to loans or insurance. It said it was also unclear whether data providers, tech developers or financial firms would be held responsible when things went wrong.

The ARISE framework would provide the needed guardrails, that consider aspects like assessments of security in AI based or partially based systems. It would provide reasoning for the cause and effect chains, as well as policies that could help secure them. ARISE would provide indicators both technical and policy based to address these issues. The UK’s financial industry would almost certainly benefit from applying the ARISE framework to their AI-based systems.

https://noma.security/blog/geminijack-google-gemini-zero-click-vulnerability/#:~:text=A%20GeminiJack%20Executive%20Summary,traditional%20security%20tools%20were%20triggered.

How do ARISE and the Diamond Threat Model compare?

As I was typing this month’s Signal, I started to ponder this question. The Diamond Threat Model is about 12 years old now, whereas ARISE is brand-new. Here are some thoughts:

Dimension	**ARISE**	**Diamond Model**
Primary goal	Produce assessed intelligence judgments	Model and analyze cyber intrusions/adversary activity
Core question	“What do we assess is happening or likely, and with what confidence?”	“Who attacked whom, how, and why?”
Orientation	Strategic / estimative	Operational / tactical
Typical audience	Policymakers, senior leaders	SOCs, CTI teams, incident responders

Aspect	**ARISE**	**Diamond Model**
Output	Judgments with confidence	Structured event analysis
Handles uncertainty	Explicitly	Implicitly
Probability statements	Common	Rare
Supports foresight	Strong	Limited
Supports attribution	Indirect	Strong

Weaponizing AI

According to a recent article from the Associated Press published by Security Week, militant groups are experimenting with AI technology. For the moment, we assess this risk to be low, as the barrier to entry for understanding how tools like ChatGPT work is low, understanding how to weaponize the technology requires a greater and deeper understanding of its inner workings. However, this does not mean that militant groups will not put in the time and effort to achieve even basic effects, which could have a wide range of impacts. AI reduces the need for organized training and reduces the overall cost barriers associated with state-sponsored R&D programs. Militant groups will almost certainly use AI for deepfake imagery, and recordings. Historically, militant groups (terrorist organizations) have used new technologies for recruiting, messaging, and media fabrications. We assess with high confidence that while militant groups will take longer to use advanced features of AI (i.e.: Agentic AI), they will find creative ways to use the technology to spread ideological messages, as well as for basic disruptive purposes. However, not regulating this technology and irresponsibly releasing it could result in lower barriers to entry for non-state actors (militant or terrorist groups) to use AI to provide instructions on how to create CBRN weapons.

https://www.securityweek.com/militant-groups-are-experimenting-with-ai-and-the-risks-are-expected-to-grow/

Secure
&
Responsible
Technology.

YOU’RE BUILDING THE FUTURE. DON’T LET EMERGING RISK STALL YOUR MOMENTUM.

SALES@ASSESSEDINTELLIGENCE.COM
EMEASALES@ASSESSEDINTELLIGENCE.COM