



AI TECHNOLOGIES

Everyone Is Adding AI. Few Are Asking What It Adds to Their Risk.

Predictive maintenance. Automated inspection. Decision support for logistics and intelligence. AI is moving into defence and aerospace fast, often through a vendor's roadmap rather than a deliberate decision by the organisation using it. Few of those systems arrive with a clear answer to a simple question: what happens if someone feeds it bad data on purpose.



The Real Exposure.

Where AI touches decision support or autonomous systems, that is not a footnote. It is a risk that needs assessing before a capability is signed off, not after.

01

Adversarial attacks on machine learning

A small, deliberate change to an image or a sensor feed has been shown to fool classification systems in ways a human observer would never miss.

2018

In 2018, researchers at the University of Michigan and the University of Washington showed that a handful of small stickers placed on a stop sign could make a computer vision system read it as a speed limit sign, reliably, from multiple angles and distances. Nothing about the sign looked wrong to a person walking past it.

02

The kind of failure a standard security review will not catch. —



Why It Matters at AAD

Defence and aerospace organisations face a harder version of a problem every industry is now dealing with: AI capability is arriving faster than the governance needed to control it, and in this sector the stakes for getting that wrong are higher than most. We help organisations build the assessment and governance layer before the capability goes live, not as an afterthought once something has already gone wrong.

03

What did we do?

Our AI practice sits alongside our cybersecurity and governance work rather than apart from it, because in practice the two cannot really be separated.



AI risk and governance assessments, covering data provenance, model integrity and accountability for automated decisions.



Adversarial testing of machine learning systems, probing for failure modes a standard security review will not find.



Secure AI adoption roadmaps for organisations evaluating vendor AI tools before they reach production.



Policy and governance frameworks for responsible AI use, aligned with emerging international standards

The organisations that get hurt by AI are rarely the ones asking too many questions before they adopt it. They are usually the ones who assumed the vendor had already asked those questions for them.

DISystems – cybersecurity and GRC advisory across South Africa, the SADC region and internationally, in partnership with **Cyberantix™**

CONTACT US AT:
tsepang@disystems.co.za
 to setup a time for more details.

