

REPORT



IM_

AI in defence and security

AI matters when it delivers in operations

Defence organisations are under growing pressure to acquire, field, and sustain new capabilities at pace.

AI can improve how data is used, reduce avoidable friction, and help people make more informed decisions.

Its value depends on how well it fits operational needs, security requirements, existing systems, and the people responsible for using it.



Three forms of AI – and what they require in defence

Traditional AI

Uses structured data to identify patterns, support forecasting, and optimise decisions. In defence, it can support areas such as maintenance planning, logistics, risk sensing, and resource allocation.

Generative AI

Works with text, images, and other unstructured information. It can support search, document analysis, reporting, and knowledge work when used in secure and well-governed environments.

Agentic AI

Combines language models with controlled access to tools and systems to carry out multi-step tasks. Its use requires clear boundaries, defined accountability, and human control.

The more autonomous the system, the more important governance, human oversight, and operational accountability become.

AI is becoming part of defence capability

AI is already being applied across defence and security, from document analysis and staff support to cyber, procurement, maintenance, and planning.

Defence organisations are building these capabilities in different ways and at different speeds. The common task is to move from promising applications to solutions that can be used securely, reliably, and with clear accountability in operations.

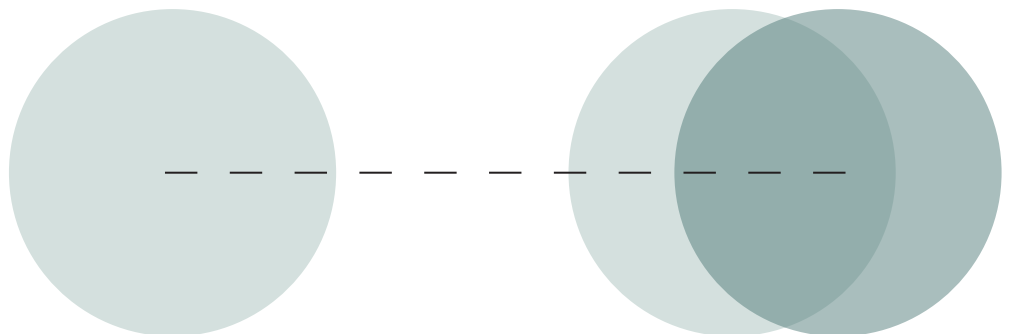
Where AI is already being applied

- Document analysis and retrieval
- Staff support
- Cyber analysis
- Procurement support
- Maintenance and availability
- Planning and simulation

What makes it operationally useful

- Usable data
- Secure environments
- Integration with existing systems
- Clear ownership
- Human oversight
- Skills and adoption

AI can create value when it helps strengthen readiness, supports informed judgement, and works reliably in operations.



From pilots to operational use

AI is being explored across defence, from document analysis and staff support to cyber, procurement, maintenance, and planning.

The next task is to bring the most useful applications into everyday work without compromising security, accountability, or operational control.

What shapes the path to scale



Sources: Implement Analysis (2026), Rand (2024), Stanford HAI AI Index Report (2025), MIT CISR Enterprise AI Maturity Model (2024)

Scaling AI means building the conditions for operational use

- Secure access
- Usable data
- Clear ownership
- Continuous learning

→ The aim is not more pilots; it is AI that can be used reliably in operations.

Where AI can support defence capability

AI is already being applied across defence and security in a number of practical areas. The most useful use cases start with a clear operational problem and can be introduced where the right security, data, and governance conditions are in place.

	Use case	What it can support
01. Procurement and logistics	Procurement support	Secure tools that help teams find approved information, prepare procurement material, and manage routine purchasing tasks.
	Supplier and supply-chain risk sensing	Data-led monitoring that can help identify supplier dependencies, bottlenecks, and emerging risks.
02. Readiness and sustainment	Predictive maintenance and spare-parts planning	Using maintenance and asset data to identify likely failures, plan work, and improve the availability of equipment.
	Availability modelling and maintenance support	Scenario modelling and digital support that can help maintenance teams plan interventions and make better use of specialist time.
03. Knowledge and staff work	Secure search, document analysis, and retrieval	Retrieval, summarisation, and drafting support across approved material, with source traceability and human review.
	Support for staff work and analysis	Tools that help staff and analysts organise information, prepare reports, and focus their time on tasks that require judgement.
04. Cyber defence	Incident triage and forensics	AI-assisted prioritisation and analysis of alerts, incidents, and device data, with clear escalation paths.
	Threat analysis and vulnerability management	Support for identifying patterns, prioritising vulnerabilities, and tracking risks across complex data environments.

→ Some use cases are ready for controlled deployment today. Others depend on further work on data, integration, security, and operating models.

Selected AI use cases in defence and security

AI can support defence capability in a number of practical areas. The strongest use cases address clear operational needs and can be introduced within secure, well-governed operating conditions.

01. Procurement support	Helping procurement teams find approved information, prepare material, and manage repeatable tasks in secure environments. Most useful where work is document-heavy, policy-bound, and subject to clear human review.
02. Readiness and sustainment	Using maintenance, asset, and spare-parts data to support planning, prioritisation, and equipment availability. Value depends on reliable data, integration with maintenance workflows, and clear ownership in the sustainment organisation.
03. Secure knowledge and staff support	Supporting search, retrieval, summarisation, and staff work across approved information sources. Useful where permissions, source traceability, and human review are built into the way the tool is used.
04. Cyber triage and analysis	Helping analysts prioritise alerts, identify patterns, and investigate incidents across large and complex data environments. The aim is to support judgement and escalation, not to replace the people responsible for cyber defence.

→ The most useful starting points are clear operational problems, available data, and the conditions needed to use AI reliably.



Selected Implement examples

These examples show how Implement has helped clients apply AI in regulated and asset-heavy environments. They illustrate several of the conditions that also matter in defence and security: trusted data, operational ownership, human oversight, and the ability to integrate new tools into existing work.

AI-supported regulatory compliance

A client in a highly regulated industry needed a faster and more consistent way to assess frequent regulatory changes across jurisdictions.

We designed a generative AI workflow that screens updates, identifies relevant changes, and supports human review.

Impact

- 50% faster regulatory review processes
- 50%+ reduction in early compliance labour costs
- Improved consistency and a more proactive compliance approach

Regulated environment

Human oversight

Predictive maintenance for heavy marine assets

Working with engineering and data-science specialists, we tested purpose-built sensors, established a reliable data pipeline, and developed an AI model to predict lubrication-related failure risks in large marine engines.

The work created a feasible route towards an onboard predictive maintenance model.

Impact

- Purpose-built sensors validated in the target machinery environment
- Reliable, continuous data pipeline
- Sensor data transformed into AI-ready features
- A feasible route towards an onboard predictive model

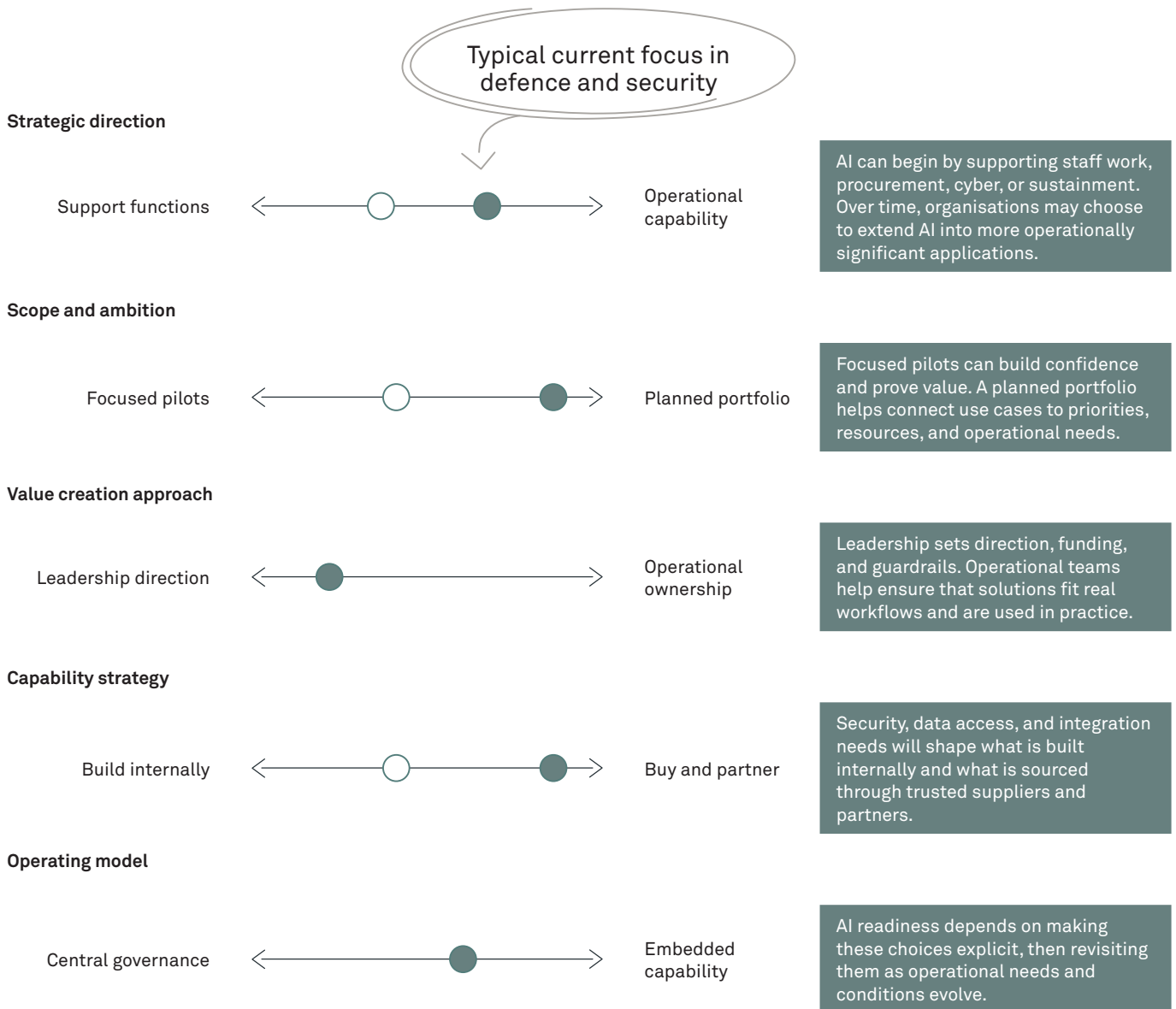
Equipment availability

Predictive maintenance

Different contexts. Similar conditions for operational use.

Five strategic choices for AI readiness

AI readiness depends on the choices organisations make about purpose, scale, ownership, sourcing, and operating model.



→ There are no universal answers. What matters is making the key choices explicit, understanding the trade-offs, and revisiting them as operational needs evolve.



Future outlook

Near term: Build confidence through practical use

AI can support document analysis, procurement support, and staff work in secure environments. These applications can improve access to approved information, reduce repeatable manual work, and help organisations build confidence in how AI is used.

Medium term: Scale secure operational use

Predictive maintenance, supply-chain risk sensing, and AI in classified environments require more than an individual use case. They depend on reliable data, secure infrastructure, clear ownership, and the ability to integrate new tools into daily operations.

Long term: Strengthen readiness and decision support

AI is likely to play a growing role in sensing, analysis, planning, and decision support. Its value will depend on whether organisations can retain human judgement, clear accountability, and operational control as use becomes more consequential.

The organisations that build these foundations now will be better placed to use AI where it can make a practical difference to readiness.

From AI ambition to operational use

We help organisations identify where AI can help, create the conditions for use, and embed it in everyday operations.

How we work

AI strategy and readiness

- Clarify where AI can support readiness, availability, staff work, and decision-making
- Set priorities, decision rights, and a practical path from ambition to use

Use case discovery and testing

- Identify operational problems where AI can create practical value
- Test selected use cases with users, operational owners, and specialists

Technology and sourcing

- Assess model, platform, architecture, and hosting options, including where secure or local deployment is needed
- Choose suppliers and partners that fit security, data, integration, and operational requirements

Programme and implementation

- Establish governance, ownership, and delivery structures needed to move beyond pilots
- Coordinate use cases, technology providers, and implementation partners

Secure deployment and integration

- Bring AI into existing systems and workflows with secure access, clear handovers, and the right deployment setup
- Address classification, compliance, testing, assurance, and operational risk

Adoption and capability building

- Prepare users and managers to work with AI in practice
- Build internal capability and feedback loops that keep solutions useful over time



Practical AI that supports people and works reliably in operations.



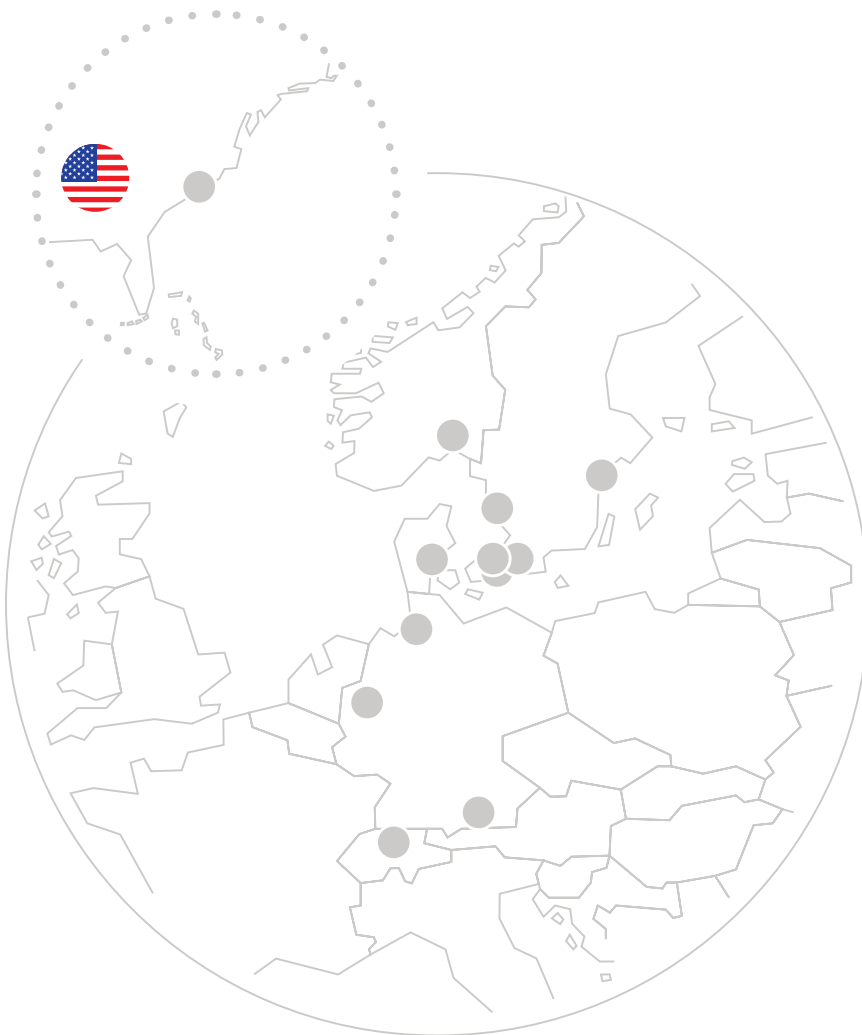
Local roots, global perspective

Founded in Denmark and built internationally, Implement combines Scandinavian roots with experience from complex transformation across Europe and the United States.

In defence and security, we help public authorities, defence organisations, and companies turn investment and ambition into capability that works in practice.

Our work spans programme leadership, organisational capability, data and technology, industrial collaboration, and implementation.

We help strengthen the links between procurement, people, industry, data, and operational use, so new capability can be brought into service, sustained, and improved over time.



- Founded in Denmark in 1996
- Partner and employee owned
- 12 offices in six countries
- Working across Europe and the United States

Contact

For more information, please contact:

Violaine Michel Lange

Implement Consulting Group

+45 60 84 90 81

vila@implement.dk

Morten Bæk

Implement Consulting Group

+45 22 88 9479

moba@implement.dk

Anders Rømer Skøtt

Implement Consulting Group

+45 31 71 74 87

anrs@thetechcollective.eu

Mads Bang-Nielsen

Implement Consulting Group

+45 26 53 16 23

mabn@implement.dk