Policy Paper

Establishing a National Sovereign AI Lab for Defence Readiness, Strategic Autonomy, and National Resilience

A mock policy paper for national defence ministries, with practical guidelines for policymakers, researchers, and military personnel.

Purpose

This paper outlines why a national defence ministry should establish a sovereign AI lab, what that institution should contain, how it should be governed, which defence use cases should be prioritised first, and what implementation principles should guide secure deployment.

It is designed as a practical policy companion to a shorter website article and can be adapted into a ministerial brief, concept note, cabinet memorandum, or institutional white paper.

Prepared for	National Defence Ministry / Security Leadership
Document type	Mock policy paper
Audience	Policymakers, researchers, military personnel, defence technologists
Focus	Sovereign AI capability, defence governance, readiness, secure deployment

Executive Summary

Artificial intelligence is rapidly becoming part of the strategic infrastructure of national power. For defence ministries, the key issue is not simply whether to adopt AI tools, but whether critical AI capability will remain trusted, secure, and available under national control during crisis, sanctions, cyber pressure, or regional conflict.

A national sovereign AI lab can address that challenge by combining assured compute, secure data environments, mission-specific model development, testing and assurance, and a long-term talent pipeline. Properly designed, it becomes a defence-readiness institution: one that improves resilience, reduces external dependence, and enables responsible military use of AI in intelligence support, cyber defence, logistics, maintenance forecasting, and strategic planning.

This paper recommends a phased national approach: begin with governance, secure pilot infrastructure, and a limited number of high-value use cases, then expand toward an enduring whole-of-defence capability.

1. Strategic Context

AI capabilities increasingly depend on access to advanced compute, secure data, trusted supply chains, and institutional capacity. At the same time, governments are treating advanced semiconductors, model capability, and compute infrastructure as matters of national security and strategic competition. This means that defence ministries must think of AI less as an outsourced software service and more as a layered national capability.

Contemporary security competition also extends beyond conventional battlefield operations. Cyber disruption, influence operations, infrastructure pressure, and strategic technology controls are now part of the broader operating environment. In such conditions, dependence on externally controlled AI systems can become a defence vulnerability.

2. Policy Objective

The policy objective is to establish a sovereign AI lab under the authority of the Ministry of Defence that can securely support defence-priority AI workloads, protect sensitive datasets, develop or adapt mission-specific AI systems, and ensure disciplined assurance and monitoring before and after deployment.

3. What a Sovereign AI Lab Should Include

- **Assured compute capacity:** secure domestic or nationally governed compute for sensitive workloads and priority national missions.
- **Secure data environments:** classification-aware storage, provenance controls, encryption, segmentation, and auditability for defence data.
- **Mission-specific model adaptation:** the ability to fine-tune, evaluate, govern, and deploy models suited to national languages, doctrine, terrain, and mission needs.
- **Assurance and red-teaming:** pre-deployment testing, adversarial evaluation, incident review, and post-deployment monitoring.
- **Talent and partnerships:** a pipeline spanning military personnel, civil servants, researchers, and trusted industrial partners.

4. Priority Defence Use Cases

The lab should initially focus on practical use cases with clear operational value and manageable risk.

- Intelligence fusion and summarisation
- Cyber incident triage and analyst support
- Predictive maintenance for defence assets
- Logistics forecasting and mobilisation planning
- Multilingual analysis and secure knowledge retrieval
- Disinformation and information-integrity monitoring
- Scenario simulation and contingency support
- Secure internal copilots grounded in approved defence documents

5. Governance Model

The sovereign AI lab should report to a Defence AI Steering Council chaired by a senior ministry leader and supported by representatives from operations, intelligence, cyber, legal, procurement, research, and security assurance functions.

Function	Role
Steering Council	Set priorities, approve deployment categories, allocate resources, review risk and assurance re
Chief Technical Lead	Oversee infrastructure, model lifecycle, evaluation pipelines, and integration architecture.
Security and Data Office	Enforce data governance, access controls, provenance, classification handling, and audit loggi
Assurance / Red Team Unit	Conduct testing, challenge assumptions, assess robustness, and monitor incidents.
Mission Owners	Define operational requirements, success metrics, fallback procedures, and human-accountab

6. Core Policy Principles

- Treat AI as strategic infrastructure rather than ordinary software procurement.
- Keep sensitive defence data in controlled national environments.
- Use AI first for decision support, not decision replacement.
- Mandate testing, monitoring, and human accountability for critical functions.
- Build modular architectures to reduce lock-in and improve resilience.
- Maintain fallback procedures for degraded or denied environments.

7. Implementation Roadmap

Phase	Indicative timeline	Key actions

Foundation	0-12 months	Create governance authority; identify first 3 use cases; establish secure pilot environme
Pilot and validation	12-24 months	Launch pilots in cyber, intelligence, and logistics; perform red-teaming; develop data pip
Operational expansion	24-48 months	Scale successful systems to more commands; stand up secure model registry; formalis
Strategic maturity	48 months onward	Integrate into wider defence planning; mature evaluation frameworks; update infrastruct

Guidelines for National Defence Ministries

The following guidelines are intended to be practical. They can be adapted into ministerial directives, AI governance frameworks, acquisition requirements, or implementation checklists.

Strategic

- Treat sovereign AI capability as part of defence readiness, alongside secure communications, cyber defence, and intelligence systems.
- Define clearly which AI functions are mission-critical and which can rely on external commercial services.
- Prioritise a limited number of defence use cases that can show measurable value within 12-24 months.

Governance

- Create a Defence AI Steering Council with decision rights over risk classification, deployment authorisation, and oversight.
- Require model cards, data lineage records, evaluation reports, and accountable mission owners for every production system.
- Review AI policies annually as geopolitical and technical conditions change.

Security

- Keep sensitive defence data in controlled environments with segmentation, encryption, strong identity controls, and auditable access.
- Mandate red-teaming and adversarial testing for prompt abuse, spoofing, data poisoning, and model misuse.
- Prepare manual fallback procedures for critical workflows in case AI systems degrade, fail, or are denied.

Operations

- Use AI first to assist analysts, planners, and maintainers rather than replacing accountable human judgement.
- Separate deployments by classification level and mission sensitivity.
- Ground internal defence copilots only in approved sources, with logging and restricted retrieval.

Procurement and ecosystem

- Include data residency, portability, auditability, continuity support, and sovereignty clauses in procurement contracts.
- Avoid avoidable lock-in by favouring modular design, open interfaces, and evaluation portability.
- Build a domestic talent ecosystem through defence-university programmes, fellowships, and trusted industry partnerships.

Conclusion

A sovereign AI lab is not simply a technology project. For a defence ministry, it is an institutional mechanism for preserving strategic autonomy, protecting sensitive data, improving operational resilience, and ensuring that critical AI capability can be governed under national authority. In an era of geopolitical uncertainty, hybrid threats, and rapid AI diffusion, this capability increasingly belongs inside the core architecture of national defence.

Reference Section for Policymakers, Researchers, and Military Personnel

1. UK Government. *UK Compute Roadmap* (2025). https://www.gov.uk/government/publications/uk-compute-roadmap/uk-compute-roadmap

2. NATO. *Emerging and Disruptive Technologies* (updated 2025). https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies

3. NATO. *Summary of NATO's Revised Artificial Intelligence Strategy* (2024). https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

4. NIST. *AI Risk Management Framework*. https://www.nist.gov/itl/ai-risk-management-framework

5. NIST. *Challenges to the Monitoring of Deployed AI Systems*, NIST AI 800-4 (2026). https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-4.pdf

6. CISA, NSA, FBI, ASD ACSC, NCSC-UK, and partners. *AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems* (2025). https://media.defense.gov/2025/May/22/2003720601/-1/-1/0/CSI_AI_DATA_SECURITY.PDF

7. U.S. Bureau of Industry and Security. *Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Semiconductor Export Controls* (2025). https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens

8. U.S. Bureau of Industry and Security. *Commerce Strengthens Restrictions on Advanced Computing Semiconductors* (2023), with related BIS updates on advanced semiconductors and AI. https://www.bis.gov/press-release/commerce-strengthens-restrictions-advanced-computing-semiconductors-semiconductor-manufacturing-equipment

9. UK Government. *AI Opportunities Action Plan: One Year On* (2026). https://assets.publishing.service.gov.uk/media/697a36873c71d838df6bd400/ai_opportunities_action_plan-one-year-on.pdf