



Dstl R-Cloud
Commercial Services
Porton Down
Salisbury
Wiltshire
SP4 0JQ

E-mail: dstlrcloud@dstl.gov.uk

Statement of Requirement for the R-Cloud Artificial Intelligence and Data Science (AI&DS) Strategic Capability

Introduction

The Defence Science and Technology Laboratory (Dstl), which is part of the UK Ministry of Defence (MOD), is refreshing its commercial agreement for Science and Technology (S&T) research contracts, known as R-Cloud (Research Cloud).

MOD places extensive fundamental, experimental and applied research with industry and academic suppliers and wants to broaden access for this supply base, reducing the cost of trading with MOD and enabling agile contracting. R-Cloud complements MOD's other contracting mechanisms and academic and industry suppliers of S&T research are now invited to apply to join MOD's research supplier community within the Artificial Intelligence and Data Science (AI&DS) Strategic Capability.

This statement of requirement relates to suppliers joining R-Cloud within the AI&DS capability area. R-Cloud provides a low barrier to entry for potential suppliers and offers direct access to MOD's current and future research requirements. Academic and industrial suppliers of Artificial Intelligence and Data Science (AI&DS) research are invited to apply to R-Cloud if you are a supplier of Science and Technology Research in this area.

The Ministry of Defence (MOD) seeks to work with industry and academic suppliers to develop, assess, integrate and exploit Artificial Intelligence and Data Science capabilities for defence and security.

Artificial Intelligence and Data Science are critical enabling technologies for modern defence. They support the exploitation of complex data, increase the speed and quality of decision-making, enable new forms of human-machine teaming, improve the efficiency of enterprise functions, and enhance operational effectiveness across multiple domains.

- Artificial Intelligence includes techniques that enable computer systems to perform tasks normally associated with human intelligence, including perception, learning, reasoning, planning, language understanding, optimisation, creativity, prediction and autonomous adaptation.
- Data Science enables the acquisition, management, integration, analysis, visualisation and dissemination of data to generate insight and support decisions.

Both Artificial Intelligence and Data Science are ubiquitous enabling technologies that are relevant to all defence and security capabilities especially command and control, intelligence analysis, autonomous platforms, computer network defence, countering deception and misinformation, sensing, defence logistics, policing and security and streamlining back-office



AI & Data
Science

functions. For a deeper discussion see the Dstl Biscuit Book (<https://www.gov.uk/government/publications/the-dstl-biscuit-book>).

This could include developing novel AI&DS algorithms, the application of AI&DS technology to domains and establishing processes and ways of working to engineer and deploy AI&DS in practical military environments.

Owing to the rapid evolution of technology in this area and multi-disciplinary nature of research in this strategic capability area, it is important to note that MOD is increasingly seeking to work in a highly collaborative and agile manner with a wide range of suppliers. Suppliers will need to have the capacity and mindset that allows for increased working in joint government / industry / academic teams and operating with multi-disciplinary skill sets and reducing transactional working. A blend of expertise from military experts, analysts, AI&DS scientists, software engineers, those with user experience and scrutineers, coupled with an agile delivery approach, will make for better outcomes.

The following areas indicate the types of Artificial Intelligence and Data Science research, development, engineering and experimentation that MOD may wish to contract through R-Cloud.

AI and Data Science Innovation and Research

MOD may seek research into novel, high-performing and robust AI and machine learning techniques suitable for defence and security applications. This may include, but is not limited to, the topics below:

- supervised, semi-supervised, unsupervised and reinforcement learning; probabilistic and causal models; graph-based methods; multi-agent systems; optimisation methods; hybrid symbolic and statistical AI; and approaches to learning from sparse, uncertain or incomplete data.
- foundation models, large language models, multimodal models and generative AI systems, including their adaptation to defence use cases. This may include fine-tuning, retrieval-augmented generation, model compression, synthetic data generation, prompt engineering, tool-using agents, automated reasoning, and methods to improve reliability, factuality and controllability.
- natural language processing and conversational AI to support interaction with defence systems, operational data, doctrine, intelligence reporting, engineering records and enterprise information. This includes systems able to support analysts, planners, decision-makers and operators while remaining transparent about uncertainty, provenance and limitations.
- novel approaches to computer vision, signal processing and multimodal. This may include object detection, classification, tracking, change detection, anomaly detection, activity recognition and cross-sensor fusion.
- knowledge representation, ontologies, semantic reasoning, temporal reasoning, geospatial reasoning and data fusion. MOD is interested in approaches that combine structured and unstructured data to support situational awareness, intelligence analysis, planning and assessment.
- AI safety, robustness and assurance. This includes approaches to testing, evaluation, verification and validation of AI systems, particularly where outputs may influence operational decisions.
- human-machine teaming, including trust, explainability, cognitive workload, automation bias, user confidence, decision support, delegation, supervision and



meaningful human control. Human-centred AI, interaction design, visualisation and cognitive systems remain important areas of interest.

AI and Data Science Engineering and Applied Science & Technology

MOD may seek suppliers able to engineer AI and Data Science systems from concept through to prototype, demonstrator or deployable service. This includes, but is not limited to, the topics below:

- requirements capture, data engineering, model development, software engineering, system integration, user-centred design, testing, assurance, deployment and sustainment.
- the development of data pipelines and architectures to acquire, manage, curate, label, store, govern and exploit data. This includes data quality assessment, metadata management, provenance, lineage, access control, interoperability, data standards and secure sharing across MOD, wider government, allies and partners.
- engineering approaches for machine learning operations, large language model operations and analytic pipeline management. This may include reproducible workflows, model registries, automated testing, monitoring, deployment, auditing, performance management and maintenance of AI systems through life.
- secure deployment of AI capabilities in cloud, edge, hybrid, disconnected, degraded or contested environments. This includes low size, weight and power AI, efficient inference, model distillation, federated learning, privacy-preserving analytics and operation under bandwidth, latency, security and compute constraints.
- Integration of AI into existing defence systems, including legacy platforms, constrained computing environments, command and control systems, intelligence tools, autonomous systems, cyber systems, engineering systems and logistics applications. This may require novel approaches to interoperability, modular architectures, open standards and secure interfaces.
- AI-enabled decision support, planning, scheduling, optimisation and wargaming. This includes support to tactical, operational and strategic planning; logistics optimisation; force generation; mission rehearsal; resource allocation; and assessment of alternative courses of action.
- ethical, legal, regulatory and policy-informed engineering of AI systems. This includes mechanisms for auditability, accountability, transparency, contestability, bias mitigation, safety cases, accreditation and responsible use. Suppliers may be required to support assurance arguments for AI systems embedded within wider socio-technical capabilities.
- techniques to detect, understand and counter AI-enabled deception, misinformation, disinformation, synthetic media, cyber threats and manipulation of information environments are also relevant. This includes both technical detection methods and human-centred approaches to presenting evidence and uncertainty to decision-makers.

Experimentation and Exploitation

MOD may seek suppliers to design, conduct and analyse experiments involving AI and Data Science concepts in simulated, synthetic, laboratory, field and operationally representative environments. Experiments may assess technical performance, operational utility, human factors, risks, limitations and routes to exploitation.



AI & Data
Science

Development of benchmarks, scenarios, metrics and evaluation methods for AI systems, including generative AI and foundation models, may be required. This includes evaluation of accuracy, robustness, reliability, latency, usability, explainability, security, safety, resilience and mission impact.

Modelling, simulation, digital twins and synthetic environments may be used to generate evidence for AI-enabled capability. This may include simulation-based training, synthetic data generation, rare-event testing, human-in-the-loop experiments, hardware-in-the-loop testing and evaluation of autonomous or semi-autonomous behaviours.

Practical exploitation of AI and Data Science may be required across defence and security use cases, including intelligence analysis, imagery analysis, cyber defence, sensing, logistics, engineering support, information advantage, autonomy, command and control, training, medical support, personnel functions and back-office efficiency.

MOD may seek methods to deploy, monitor, update and sustain AI capabilities in use. This includes approaches to model drift, adversarial adaptation, changing data distributions, user feedback, continuous assurance, incident reporting, rollback, retirement and through-life management.

Support may also be required to develop Concepts of Employment, Concepts of Operations, doctrine, training implications and Defence Lines of Development for AI-enabled capabilities.