



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

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.

MOD seeks to increase its exploitation of Artificial Intelligence (AI) and Data Science (DS) to address a wide range of defence and security challenges in a manner that is safe, ethical & responsible.

- Artificial Intelligence refers to a broad spectrum of techniques that enable computer systems to perform tasks that typically require human intelligence. These include: learning and adaptation; sensory understanding and interaction; reasoning and planning; optimisation of procedures and parameters; autonomy; creativity; and extracting knowledge and predictions from large, diverse digital data.
- Data Science is a multi-disciplinary field that enables the discovery of insights from data. Acquiring, processing, managing, correlating, visualising, drawing insights from and disseminating data from different sources to provide information and intelligence to a decision maker is a critical enabler for all military and security operations. It ensures that the best informed decisions are made at the right time based on the right data.

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 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.

Through such rainbow teams, it is anticipated that the suppliers will develop skills and attributes necessary for such AI- and DS-based work within the defence and security environments. The suppliers should be able to demonstrate and mature their skills (including operating in client-facing situations, being able to structure AI&DS problems, handle agile development of AI&DS systems via scrum management etc.).

Below is a summary of overarching research requirements for AI&DS encompassing the programme areas of Artificial Intelligence and Data Science.

Artificial Intelligence and Data Science – Statement of Requirement

Artificial Intelligence and Data Science, including its tools and the hardware to effectively execute them, is a critical enabler for military capability to deliver sophisticated effects and assist with increasing the speed of decision-making as part of a human-machine team, at all levels. The research into AI&DS will help to deliver a critical capability for defence and security that offers a competitive edge in a manner that is moral & ethical, reinforces international norms and counters the irresponsible use of AI&DS.

1) The scope of coverage of topics related to AI&DS Innovation and Research topic includes, but is not limited to, the following:

- a) Developing high performance and robust AI and machine learning techniques suitable for defence and security applications, for example
 - Developing innovative new AI and machine learning algorithms as well as improving the performance of existing algorithms including supervised, semi-supervised, unsupervised & reinforcement learning, generative adversarial networks, multi-agent systems, fuzzy systems, model- and case-based reasoning, search algorithms, and graph neural nets etc.
 - Research into AI topics such as broad AI, transfer learning, context-aware learning, data sparse learning (e.g. one shot, few shot or synthetic learning) and Bayesian networks.
 - Creating new approaches for Natural Language Processing for effective engagement with military personnel in complex environments.
 - Computer vision techniques for detecting, recognising and classifying real-world objects based on a variety of sensor modalities (including electro-optic, acoustic, thermal, radar, and lidar).
- b) Demonstrating novel approaches to managing data and extracting knowledge from complex heterogeneous datasets



AI & Data
Science

- Developing ontologies, knowledge representations and reasoning approaches that are applicable to defence and security domains.
 - Application of novel computing architectures, e.g. clouds, clusters and edge-based processing, to conduct various facets of Data Science.
 - Developing new techniques for topics such as hypothesis generation, data fusion and correlation and prediction of data from diverse sources.
 - Understanding, managing, quantifying and communicating uncertainty in AI&DS systems so that users can investigate uncertainty and its effects in every part of the system, from data in, through learning and processing, to outputs, and its impacts.
- c) Developing the next generation of AI hardware to enable high performance and new approaches to data processing
- Developing high performance processors with low size, weight & power characteristics to enable “AI at the edge”.
 - Researching novel / next-generation (e.g. neuromorphic, quantum, optical) technologies to enable new processing approaches.
 - Developing novel programming techniques, methodologies, and tools to develop AI&DS solutions.
- d) Developing understanding regarding how to improve the performance of Human Machine Teams
- Research into how to form effective and trustworthy human-machine teams.
 - Devising cognitive systems that effectively emulate human activities in order to automate workflows and increase the tempo of activities within these workflows.
 - Underlying research into providing Explainable Artificial Intelligence, particularly for novel forms of machine learning.
 - Techniques and guidelines for Forming, Storming and Norming effective and trustworthy human-machine teams.
 - Developing human-centred Artificial Intelligence and Data Science to support information interaction, visualisation and cognition.
 - Situational Awareness and Understanding models, processes and representations based on AI for managing the battlespace, ISTAR operations and undertaking ‘what-if’ analysis for mission planning and force optimisation.
 - Agile adaptation and employment of AI-based user facing applications and services.
- e) Conducting basic research into Test, Evaluation, Verification and Validation to ensure AI&DS solutions are safe and robust for defence and security applications
- Conducting basic research to underpin tools and techniques that are able to accredit AI and machine learning algorithms in safety critical systems.
 - Developing new approaches to assess the performance and robustness of AI&DS techniques against a wide range of defence and security systems.
 - Researching and understanding potential vulnerabilities in AI and DS systems in order to develop countermeasures, for example to data poisoning or adversarial attacks.

This may include, but is not limited to:

- Basic research into processes, techniques and technologies that underpin AI&DS concepts.
- Innovative ideas about how military users can engage with AI&DS.
- Research and Development of Data Science systems, components and lifecycles.
- Devise new research concepts and robust methodologies for AI&DS.



AI & Data
Science

- Development of data correlation, forecasting and validation techniques and algorithms.
- Novel technologies based on bio-inspired systems that lead to new AI&DS paradigms.
- Creative ways of working, Concepts of Employment (CONEMP) and Concepts of Operations (CONOPS) for new AI-enabled MOD capabilities.

2) The scope of coverage of topics related to AI&DS Engineering and Applied S&T topic includes, but is not limited to, the following:

- a) Developing the regulations and ethics that can underpin the application of DS and AI solutions for safe, proportionate and secure defence and security capabilities
 - Technologies, procedures and strategies associated with managing and regulating the safe and secure deployments of AI&DS solutions at MOD sites and engagement with MOD people.
 - Service Orientated Architectures and micro architectures to support AI&DS development according to MOD regulatory guidelines.
 - Technologies, processes, standards and strategies to accredit and assure AI algorithms as part of the wider system that control physical objects, military workflows and vehicles, particularly when in motion or part of a mission-critical process such as a kill-chain.
 - Multi Domain Integration of effects employing both influence and kinetic activities controlled by AI, but always within a framework of meaningful human control – the UK does not research or develop lethal autonomous weapon systems. The AI is supporting a human operator in these cases.
 - Technologies to monitor and govern the moral, ethical, political and legal assurance of AI-and DS-based solutions.
- b) Constructing powerful and “easy to use” tools and techniques that support the engineering and application of AI and DS technologies
 - Application of cutting edge AI and machine learning techniques for DS and informatics.
 - Discover, manage and generate data sets in order to effectively train and test machine learning algorithms including use of techniques such as simulation and ensemble learning.
 - Automated entity extraction and pattern recognition from textual data sources.
 - Tools to understand and address the provenance and propagation of bias in data, algorithms and wider AI&DS systems.
 - System engineering approaches to the whole AI&DS ecosystem, including requirements capture, architecting, prototyping and enterprise-wide methods.
 - Understanding and improving data quality.
 - Application of ‘Big’ data analytics approaches.
 - Tools to access, manage and store data, information, knowledge and intelligence for defence and security applications.
 - Discovery and rapid assessment of emerging algorithms, programming libraries and languages and subsequent application of them to defence & security problems. This might include techniques in academic publications that require implementation and modification of existing open source code.
 - Use of AI&DS tools for constructing plans and controlling the execution of these plans including tactical-, operational- and campaign-levels across multiple disciplines and coordinating planning with other agencies.
 - Working with massive unstructured data sets, including temporal and spatial data from various sources including social media, logistics, engineering, and from deployed sensors.



AI & Data
Science

- Pioneering Artificial Intelligence and Data Science techniques (including the application of Deep Learning, Reinforcement Learning and Bayesian Methods) for tasks such as image analysis or information extraction from unstructured text.
- c) Applying new AI&DS metaphors, best practices and technologies into a spectrum of applications within the defence and security communities to support development of new systems and enhancement to legacy applications
 - Fostering collaboration and interoperability with UK MOD allies and pan-government agencies on AI topics in order to create standards and exchange of AI tools and knowledge.
 - User-driven development of AI&DS enterprise-scale and bespoke solutions, including user research, service design, interaction design and user-focussed testing.
 - Smart sensors and smart cities employing AI&DS concepts
 - AI&DS engineering “best practice” to design, develop and integrate AI&DS solutions that are scalable and can be optimised for operational performance.
 - Employing AI tools for intelligence analysis, imagery analysis and social network analysis.
 - Fundamental architectures and methodologies to combine diverse AI and DS technologies into a coherent multi-intelligence framework.
 - Pan-Defence Lines of Development (DLoD) approaches to improving AI-and DS-based capabilities including changes to concepts & doctrine, organisation, processes and training.
 - Approaches that will be employed to underpin the application of Artificial Intelligence and Data Science technologies for defence and security operational use cases including for employment in logistics management, Command and Control of assets / troops etc.
 - Application of AI concepts and implementations to enhance extant systems used by defence and security agencies for a range of purposes including anti-submarine warfare, intelligence analysis, computer network defence, platform autonomy, electronic surveillance, forensics, human performance, threat assessment, sensing, CBR (Chemical, Biological and Radiological) applications, and so forth
 - Integration of AI within virtual intelligent systems, particularly legacy systems where the hardware – upon which AI algorithms can be executed – will be constrained. Approaches are needed to cope with perhaps unchangeable elements of the legacy system, security requirements, lack of access to everything the AI algorithms might want, etc.

This may include, but is not limited to:

- Software and hardware tools and methodologies to understand how to engineer and sustain AI&DS systems, particularly those using machine learning technologies, for use in defence and security operational environments.
- Engineering of Artificial Intelligence and Data Science methodologies, techniques and tools to acquire, manage, propagate, visualise and control all data required for defence and security applications.
- Applied research into processes, techniques and technologies that may be of use to AI-enabled and data-intensive systems.
- Development of component, sub-system and system level aspects of various socio-technical systems that employ AI&DS principles.
- Ensure new ways of working and tools when handling the Big Data and Data Mining associated with harvesting data-rich military environments.



AI & Data
Science

OFFICIAL



- Upgrades for current UK MOD AI-supported platforms, systems and doctrine.
- TEV&V.
- Cloud- and Edge-based AI.
- Countering AI-based digital deception.
- Develop approaches to architect, design, implement and test AI&DS solutions in support of the above.

3) The scope of coverage of topics related to AI&DS Experimentation and Exploitation topic includes, but is not limited to, the following:

- a) Exploiting AI&DS technologies, algorithms, tools and approaches in real-world defence and security domains to provide through life capabilities
 - Routes to understand and address the provenance and propagation of bias in data, algorithms and wider AI&DS concepts in deployed systems.
 - Employ methods to access, management and storage of data, information, knowledge and intelligence for defence and security applications.
 - Data integration into capability development and sustainment lifecycle.
 - Data visualization in user journeys and experiences mapping.
 - Accreditation of deployed systems containing AI&DS elements, including security, safety and verification and validation.
 - Accreditation of deployed machine learning and deep learning solutions used in non-safety-critical systems.
 - Approaches, metaphors, guidelines, design patterns and tools to accredited AI&DS systems in safety-critical settings
 - Agile adaptation and employment of user-facing Artificial Intelligence and Data Science applications and services.
 - Application of AI&DS techniques to generate insights to defence & security challenges faced by MOD Front Line Command and end-user clients.
 - Methods to pragmatically integrate AI technologies with personnel in real military settings.
- b) Construct, plan, conduct and analyse the results of experimentation with AI&DS concepts in simulated and realistic environments
 - Design and execution of experiments to effectively test AI-and DS-related hypotheses.
 - Integration of socio-technical components to build experiments into AI&DS.
 - Use of Artificial Intelligence and Data Science principles, toolsets and experimental know-how to formulate and assess operational defence and security concepts, as well as modelling and simulating these concepts to provide evidence for business cases.
 - Assessment methods to quantify the effectiveness of AI&DS solutions within defence and security enterprises, including indicators and metrics.
 - Analysis of the results from socio-technical experiments that employ AI&DS technology.

This may include, but is not limited to:

- Maturing techniques and know-how that may be used to develop future experiments into AI&DS.
- Applied research into component, sub-system and system level equipment, processes or policy through the design, execution and analysis of experiments on AI technology.
- Develop software and hardware tools to aid the conduct of AI experiments.



AI & Data
Science

- Generation and use of synthetic data for experiments.
- Upgrades for current UK MOD AI-enabled platforms, systems and doctrine.
- Experimentation with novel Artificial Intelligence and Data Science concepts and solutions.
- Practical exploitation of AI and DS ideas into a spectrum of defence and security use cases.
- Methods and approaches (including appropriate means of assurance) to support effective and efficient reproducibility of analytic pipelines, and reuse of algorithmic functionality.
- Development of techniques for using existing non-traditional data sources in integrated Data Science solutions for legacy defence and security enterprises.
- Performance tuning and optimization of deployed systems using AI&DS.
- New methods to ensure interoperability with future suites of models. As autonomous, AI-enabled platforms become the norm MOD will need to be able to 'test' them and this is likely to involve modelling and simulation – it seems strange to recreate an autonomous agent in a simulation when you could just 'plug it in' as hardware in the loop.
- Develop approaches to deploy, refine and sustain AI&DS solutions in support of the above.