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

E-mail: dstlrcloud@dstl.gov.uk

Statement of Requirement for the R-Cloud Survivability 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 Survivability Strategic Capability.

This statement of requirement relates to suppliers joining R-Cloud within the Survivability 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 Survivability research are invited to apply to R-Cloud if you are a supplier of Science and Technology Research in this area.

Statement of Requirement

"Survivability S&T capabilities that assess the threats to our defence and security (D&S) systems and develops the measures necessary to achieve optimum survivability at an affordable cost, enabling a mission to be completed successfully in the face of a hostile man-made environment. A systems approach is taken to optimise technical and non-technical measures in order to defeat the threat weapon engagement sequence and mitigate the effects to our systems and personnel."

What follows in this statement of requirement is an introduction to the Survivability Strategic Capability, an introduction to the Survivability S&T Pipeline and an outline of the Survivability SC R-Cloud Requirement (describing typical tasks).

Introduction to Survivability - Survivability is not the same as safety. Survivability is set in a hostile environment where others deliberately try to impede what you are attempting to do, often via lethal means.

Survivability encompasses a broad range of technical areas across land, air and maritime domains, not limited to but including the following:
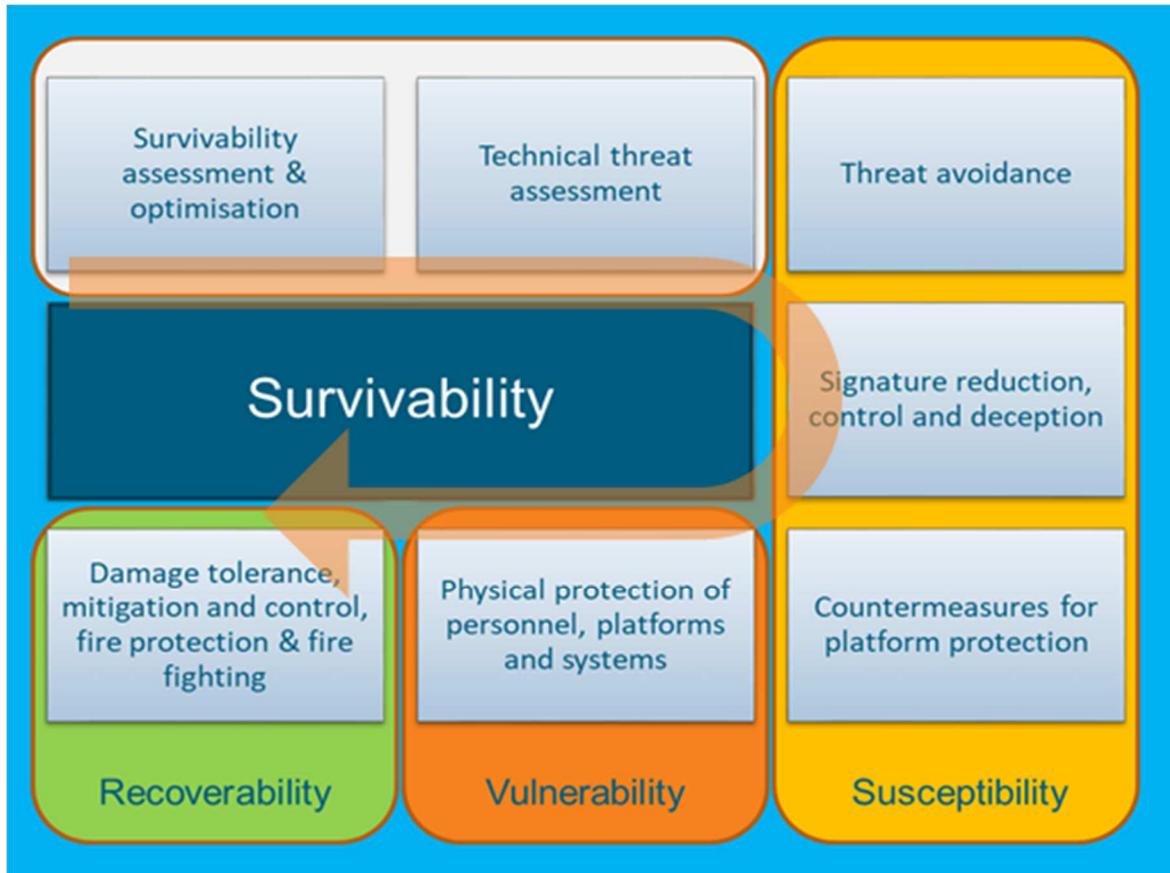
The inferred flow indicated by the arrow represents generally how the elements of survivability address the threat in progression through a typical mission. The first two elements are most often used in research and mission planning whereas those in susceptibility, vulnerability and recoverability can also be encountered in the context of operational missions. Once having successfully progressed beyond the immediate threat the survivability process begins again at susceptibility (hence perceived as a cycle).

A more detailed description of the elements of Survivability are:

TITLE	DESCRIPTION
Survivability	Survivability Science & Technology (S&T) capabilities that assess the threats to our Defence & Security (D&S) systems and develops the measures necessary to achieve optimum survivability at an affordable cost, enabling a mission to be completed successfully in the face of a hostile man-made environment. A systems approach is taken to optimise technical and non-technical measures in order to defeat the threat weapon engagement sequence and mitigate the effects to our systems and personnel.

	Survivability assessment and optimisation	S&T that enables assessment and optimisation of survivability measures against representative threats for platforms, systems and systems of systems (at the platform and force level) in a mission and multi-mission context. This draws on a wide range of survivability technology areas and other military capabilities (such as counter-fire, tactical agility, enhanced sensors & situational awareness) by consideration of the threat encounter frequency, systems balance, integration and performance assessment & assurance with trade-offs quantified in systems performance and cost-effectiveness modelling.
	Technical threat assessment	S&T that provides an exploitable understanding of threat systems, their performance and their use in typical encounters. It includes the technical analysis and characterisation of current and future D&S threats (and associated components) at a tactical level (such as Electronic Countermeasures for Counter-Improvised Explosive Devices (ECM CIED), Specialist CIED Search, Specialist Tactical Effects) to determine functionality, performance and exploitable vulnerabilities. Impact assessment of threat against deployed operational capability.
	Threat avoidance	S&T that enables exploitation of system enablers to influence threatening encounters at preferred time and place of choosing. This can be achieved through timely, high confidence and effective threat and environmental sensing of threat systems and sensors such that manoeuvre, platform agility and autonomy can be used to reduce hostile acquisition and engagement. This also includes exploitation of timely, accurate and effective fused situational awareness pictures of threat systems to avoid or minimise exposure to our platforms.
	Signature reduction, control and deception	S&T that enables confusion and degradation of enemy Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) and seeker effectiveness through suppression and manipulation of platform and force signatures and the support of deception operations. This is achieved through the application of good platform design, bespoke solutions, the integration of signature management technologies, the control of emissions relevant to their military function and passive & reactive deception measures with full consideration of counter-surveillance threats and mission requirements.

	Countermeasures for platform protection (threat warning, decoys, flares, obscurants and control systems)	S&T that enables the defeat of approaching imminent threats or that inhibit the launch of threats through bespoke solutions, the integration of systems, technologies and Tactics, Techniques & Procedures (TTPs). These include threat characterisation and exploitation of their vulnerabilities, threat sensing & approach warning, countermeasure effects, deployment and performance optimisation; development and operational test & evaluation and quantification of the performance of countermeasures against the threat set; complying with architectural requirements and constraints for tri-service host platforms, systems and system of systems.
	Physical protection of personnel, platforms and systems	S&T that reduces the terminal or lethal effect of an attacking threat thus providing physical protection of personnel, platforms and infrastructure for all environments. This is achieved through good design, bespoke solutions and the integration of technologies for physical protection by consideration of threat information, vulnerability assessment, casualty trends, operational and legal constraints, etc.
	Damage tolerance, mitigation and control, fire protection and fire fighting	S&T that reduces damage incurred by weapon attacks and their consequential effects with specific consideration of the ability of the system to recover, plus the associated impact on the platform's ability to continue to fulfil their mission and military role. This area will also specifically address firefighting and damage control.

Introduction to Survivability S&T pipeline – Survivability systems, technologies and TTPs are generally initiated, developed, evaluated, assured and introduced into Service via progression through the Survivability S&T pipeline.

Figure 1 - Survivability S&T Pipeline

Threat evaluation enables understanding of the likely challenges encountered in typical scenarios and missions. It includes technical threat assessment. These enable insights into current and emerging/novel threats, approaches to mitigate these threats and the formulation of survivability requirements.

Mitigation S&T uses the threats and mitigation insights to devise and develop sub-systems and technologies to provide counters to threats which may then be used in a mission context. These grow in maturity (with appropriate development & testing and progressing through the stages of Technology Readiness Levels (TRLs)), increasing capability, efficacy and

confidence to a point where affordable, high-credibility technologies and sub-systems can be down-selected for integration into platform systems.

Systems integration brings these credible technologies and sub-systems together into a platform system (and sometimes as system of systems) context with the required architectural, interface and common standards to ensure they can function together as desired. Hardware, software and human directed elements are tested as a system and emergent properties (often unexpected) provide insights to integrated performance and behaviours leading to further development and the evolution of TTPs.

The *procurement* and *in-service* stages are, on the face of it, self-explanatory, though typically there is considerable development of requirements and specifications before an evaluated final product is produced and accepted into Service. That development process must follow associated Defence Lines of Development (DLOD) elements such as training and logistics. During the often-long period of being in-service, military products and TTPs continue to evolve as problems, features and new requirements (driven by changes in threats, military use etc.) become evident and require minor and sometimes major upgrades.

Outline of Survivability R-Cloud requirement - This R-Cloud requirement covers a wide range of typical tasks across the full breadth of all survivability elements and the whole length of the survivability pipeline such as:-

- *Specialist advice services and decision support* – the conduct of survivability and survivability-related S&T analysis studies and simulations that provide insights and inform decisions;
- *Requirements & evaluation* – Industry and academic capabilities are needed to assist exploring and understanding the military capability needs & associated functional needs. This supports MOD to:-
  - o generate insights for specifications and conducting simulation and
  - o conduct simulation and practical experimentation to test and evaluate. This covers concepts, technologies, stand-alone and fully installed survivability performance and enables us to gather evidence for compliance and build survivability assurance.
- *Research and development* (R&D) – Most tasks are likely to include some R&D. Typical topics include the following to push the boundaries of survivability S&T:-
  - o conceptualisation, design, development, trial, testing, maintenance, modification and repurposing of
  - o techniques, tools, methods, models, hardware and software.

This covers the full range of S&T disciplines from pure sciences, applied sciences, conceptualisation, engineering and systems engineering. Examples are maths, physics & chemistry; material sciences, electro-optics (including visible, IR and UV), underwater (including acoustic and non-acoustic), software engineering (including embedded software and complex devices), Radio Frequency (RF) and electronic engineering to systems architecture development and engineering.

Requirements for the approach to Survivability tasks

During next few years, MOD anticipate that some boundaries between D&S will become less distinct. MOD aims, where appropriate, to share capabilities & knowhow (data, methods, technologies and systems) seamlessly within security constraints, to use capabilities and knowhow from outside of D&S to fill gaps, and embrace a contemporary approach to communication of findings. We strive to work with suppliers and partners new to D&S who can bring fresh ideas and perspectives.

We are looking to work with companies who are:

- New to D&S but or willing to learn enough context in order to apply ideas and conduct S&T research and studies;
- Experienced in D&S, and willing to work constructively, openly and collaboratively with other companies;
- Able to create modern, interactive and potentially sophisticated visualisations and use innovative ways to generate insights and communicate findings;
- Expert in one or more survivability-relevant methods, or have made innovations around applications of techniques;
- Willing to work with us to bring techniques into common usage (which typically requires robust demonstration and support);
- Ready to work with capabilities and knowhow of variable age, provenance and relevance and find ways to improve it for application to problems, wherever possible making improvements available for subsequent work regardless of who conducts it;
- Willing to find or generate new capabilities and knowhow and apply them to D&S;
- Prepared to constructively challenge the way MOD conducts and delivers S&T in order to drive continuous improvement for the benefit of UK
- Willing to develop our relationship, building mutual trust and confidence, and aspiring towards longer-term productive collaboration and perhaps even some assured reliance.

Requirement for application of Survivability technical capabilities

Requirements let under the Survivability R-Cloud area may require a diverse range of technical capabilities to be applied, developed or enhanced individually or in combination.

Examples of categories of techniques are:

- Systems engineering (i.e. analysis of requirements, systems concepts, system design, system assessment, systems integration, systems assurance, transition to operations)
- Operational advice support (i.e. provision of tools and techniques, modelling, laboratory and field testing, equipment evaluation, risk assessment)
- Survivability performance assessment (i.e. method development, modelling tool design, development, verification and validation, concept evaluation, survivability optimisation)
- Support to modelling, simulation and analysis tools and capabilities including the provision of advice, specialist technical support, independent technical assurance, management, review, maintenance, development and sustainment of existing and new capabilities.

- Signature assessment (i.e. computer modelling development and studies, component and integrated platform signature measurement, signature analysis and visualisation)
- Signature suppression (i.e. requirements definition, signature concept evolution, mitigation method design, development, assessment and integration)
- Countermeasure effectiveness assessment
- Countermeasure development
- Protection assessment
- Protection development
- Fundamental sensor performance modelling from first principals;
- Novel approaches to synthetic scene generation (across all bands and both in air and water);
- Development of robust, scalable and expandable testing architectures;
- R&D on updated laboratory testing equipment and approaches;
- Development and application of advanced analytical approaches, e.g. machine learning and artificial intelligence;
- Development of novel reporting methods, e.g. smart tools that can be interrogated by a human;
- Rapid and accurate translation technologies;
- Underpinning research review, e.g. horizon scanning and technology watching (including foreign language);
- Knowledge management solutions to facilitate capture and exploitation (within a unique security environment) of diverse datasets and identify trends;
- Agile access for generic forward engineering albeit using new or novel approaches, i.e. not the specific activities that are already done via EW&C;
- Enterprise architecture development, i.e. the development and application of novel approaches to capture information on and support understanding of complex military threat systems;
- Advanced approaches for storing, analysing and reporting on huge volumes of disparate data sources, i.e. our big data problem!

This list is not exhaustive. There are many techniques within each category as illustrated in the first few bullets above. Additionally there are also novel techniques that do not fall into any category; all are in scope if they can add value to Survivability-themed problems. This requirement neither places specific requirements on specialism in suppliers, nor makes constraints on technical capabilities that may be requested. However, MOD welcomes and encourages declaration of specialisms or niche-expertise by suppliers as part of the R-Cloud sign-up process.

Suppliers are required to demonstrate appropriate knowledge and expertise where requested by MOD in specific tasks. Where suppliers are proposing technical capabilities, MOD also require suppliers to be able to explain and justify their merits in the context of the specific task.