FRAZER-NASH CONSULTANCY
A KBR COMPANY

ARCD

University of Exeter

Cyber Defence Innovation Challenge

Calling all academics with potential innovations in science and technology, who can support the Autonomous Resilient Cyber Defence (ARCD) project.

Frazer-Nash is inviting interest from experts who have potential innovations in science and technology that can support the Autonomous Resilient Cyber Defence (ARCD) project.

As defence networks and systems are becoming more complex and interconnected to meet operational demands, it is becoming increasingly difficult for cyber defenders to respond effectively to incidents. In parallel, aggressors are adopting increasingly sophisticated approaches and leveraging artificial intelligence (AI) and machine learning (ML) approaches to outpace defenders.

Identifying, selecting and carrying out cyber defence responses in a machine relevant timeframe is essential to mitigate these threats. The use of AI and ML techniques are a critical defence against these attacks; research is needed to develop and mature these techniques for Defence.

ARCD is funded for four years, out to FY 24/25, and aims to research and develop self-defending, self-recovering concepts for military platforms and technologies. We are looking to engage with a broad range of suppliers and members of the academic community, particularly those with expertise who do not traditionally deliver into defence. The programme will support research, PhD's, all ideas welcome.

If you're academic that can help achieve the project outcomes of:

- Undertaking high risk, low technology-readiness level (TRL), research tasks
- Developing an ARCD Concept Demonstrator, covering:
- Autonomous threat analysis, forecasting and prediction
- Mission aware autonomous decision making, and
- Effectors for automated response

Then please sign up to the information event on **Wednesday 14th December** online to find out more and next steps.

www.fnc.co.uk/arcd

arcd@fnc.co.uk

Autonomous Resilient Cyber Defence (ARCD)

The Cyber Defence Enhancement Project

Within Dstl's Cyber Security programme, the Cyber Defence Enhancement (CDE) project represents a new opportunity and ambition to explore cutting edge Science and Technology cyber security research.

The CDE Project currently has three areas of focus:

- **Reduce the Cyber Attack Surface**, for next generation capability hardening the system by using hardware and software technologies to reduce vulnerabilities.
- **Military Systems Information Assurance**, for next generation capability protecting information using novel mechanisms and approaches.
- **Autonomous Resilient Cyber Defence**, for generation after next capability defend military operational systems at pace.

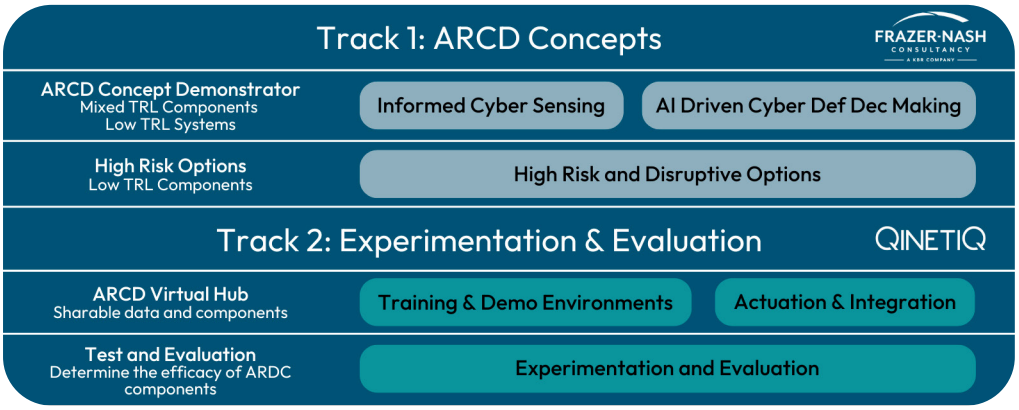
Autonomous Resilient Cyber Defence

ARCD is a four-year programme (completing March-25), which aims to develop self-defending, self-recovering concepts for military operational platforms and technologies, with an aspiration to achieve 'Full Auto' cyber defence.

At the end of year four we will demonstrate an ARCD system integrated into a representative military environment under active attack, and in doing so build an enduring capability in the UK to develop and apply research on ARCD, specifically growing Cyber and AI skills.

ARCD is being delivered through the Serapis framework, split into two tracks:

- Track 1, being delivered by Frazer-Nash, under Serapis Lot 6, will deliver the ARCD Concepts across three coordinated projects, described below.
- Track 2, being delivered by QinetiQ, under Serapis Lots 3, 4 and 5 will provide the ARCD Experimentation and Evaluation.



Track 1 ARCD Concepts

High Risk and Disruptive Options – Identify truly novel low TRL research areas that take advantage of areas where the UK is, or is poised to be, a world leader. Work with suppliers to conduct horizon-scanning to generate a high-risk/high-impact research landscape.

AI Driven Cyber Defence Decision Making – Will develop medium TRL concepts and to mature research concepts and configure existing products for integration into the concept demonstrator covering mission aware analysis and AI decision making.

Informed Cyber Sensing - To be able to respond against cyber threats, attacks need to be attributed, specifically the motivation and intent of the aggressor, enabling appropriate autonomous responses to detect, defend or deter cyber adversaries.

Dstl

Dstl is one of the principal government organisations dedicated to science and technology in the defence and security fields.

Frazer-Nash Consultancy

Frazer-Nash help organisations deliver innovative systems, engineering, and technology solutions to make lives safe, secure, sustainable, and affordable.

QinetiQ

QinetiQ is a company of scientists and engineers committed to listening, understanding, and responding to our customers'' needs.

Serapis

The Serapis framework enables Dstl, MoD and the frontline commands.to quickly and efficiently place contracts for scientific and technical research and development.

- Lot 3 – Decide
- Lot 4 – Ass Info Infra
- Lot 5 – Sim & Synth Env
- Lot 6 – Understand

HOW TO ENGAGE

For Track 1 Frazer-Nash will issue problem books to the Serapis Lot 6 Supply Chain.

We are also interested in any ideas from the supply chain or academia which can contribute to the Track 1 concepts.

If you are interested in working with Frazer-Nash to deliver the ARCD Track 1 concepts, or to find out more please email arcd@fnc.co.uk