Autonomous Resilient Cyber Defence – Intelligent Agents

Threats to UK communications, networks, and information & platform systems are growing, risking our ability to engage in multi-domain operations with allies and partners.

Safeguarding Information is the lifeblood of contemporary military operations and identifying and carrying out cyber defence in a timely manner is essential. So, the Defence and Security Accelerator (DASA) is pleased to launch a new Innovation Focus Area (IFA) called Autonomous Resilient Cyber Defence , which aims to develop self-defending cyber security systems for military operational platforms and technologies.

This IFA is being run on behalf of Defence Science and Technology laboratory (DSTL) and Defence Science and Technology (DST) and seeks proposals that will promote a shift in resilience of military systems to cyber-attacks through autonomous detection.

Can you help? Read the competition document now and submit your idea.

How much funding is available?

DASA is expecting proposals with low Technical Readiness Level (TRL 1 to 4). We have two levels of funding:

- Less than 6 month contract: up to £150K
- 6 to 12 month contract: up to 300K

Key dates

Cycle 1 of Autonomous Resilient Cyber Defence IFA is open now, and it will close on 20 October 2021. Cycle 2 will run from 20 October 2021 to 05 January 2022.

Protecting the lifeblood of military operations

Military networks and systems have become more complex and interconnected, both internally and with allies, and with commercial and civilian infrastructure.

Meanwhile, cyber attacks have become more sophisticated, with potentially more impact on military operations. The Autonomous Resilient Cyber Defence IFA aims to research and develop self-defending, self-recovering concepts for military platforms and technologies.

We are looking for technologies that:

- exploit advances in IT and Operational Technology (OT) and cyber

response and recovery approaches to develop self-defending, self-recovering concepts for military operational platforms and technologies.
- promote resilience of military systems to Cyber-attacks through autonomous detection and identification of cyber threats, to enable the Ministry of Defence (MOD) to rapidly scale cyber defence beyond that of human operators.

Read the full competition document for more on what technologies we are looking for

Key challenges

This IFA seeks to develop autonomous cyber defence agents that can respond to adversary and threat activity on networks and systems without human intervention. These autonomous agents will need to:

- operate with incomplete or uncertain data
- reason over a range of response options
- evaluate the risks and impact of selected approaches
- continuously monitor for unintended consequences
- operate in edge environments where computer capability is scarce
- can provide explainable justification for its actions

Submit a proposal!

The closing date for proposals of this IFA is 20 October 2021 at midday BST. A second cycle will run from 20 October 2021 to 05 January 2022. Click here for the full scope in the competition document and submit a proposal.

See DASA's other cyber security IFA

You might also be interested in another cyber security IFA we are running called Reducing the Cyber Attack Surface. This IFA seeks proposals that accelerate next generation hardware and software technologies to reduce the vulnerabilities within current and future computer networks and systems.