[Helping the military shrink its cyber attack surface](#)

The defence sector is diverse and continually growing, with a large integrated network of legacy cyber technologies. This presents a substantial and diverse surface area for cyber enabled attack to disrupt military operations.

Being able to accelerate next generation hardware and software technologies to phase out the cyber vulnerabilities within current computer networks is vital in order to reduce defence exposure to cyber attack.

So, the [Defence and Security Accelerator](#) (DASA) is pleased to launch a new [Innovation Focus Area](#) (IFA) called [Reducing the Cyber Attack Surface](#), which aims to develop technologies that reduce the opportunity for cyber attacks on Ministry of Defence (MOD) systems and platforms.

This IFA is being run on behalf of [Defence Science and Technology laboratory](#) (DSTL) and Defence Science and Technology (DST) and seeks proposals that enable greater confidence and a level of assurance in military systems against cyber-enabled attack.

Can you help? [Read the competition document now and submit your idea](#).

How much funding is available?

DASA expects to fund proposals within Technical Readiness Level 4 – 7 [(TRLs)](#) up to £300K for a 9 month contract. Proposed technologies should demonstrate by providing a roadmap describing how they would achieve a technical demonstrator by end of Financial Year 2023 if further funding was made available.

Key dates

Cycle 1 of the Reducing the Cyber Attack Surface IFA is open now, and it will close on 20 October 2021 at midday BST. Cycle 2 will run from 20 October 2021 to 05 January 2022.

A new generation of cyber resistant hardware and software

The MOD is interested in identifying and accelerating next generation hardware and software technologies to reduce the vulnerabilities within current and future computer networks and systems, focusing particularly on operational technologies.

We are looking for technologies that:

- intelligently apply technologies that significantly reduce the opportunity for cyber attack
- effectively raise the barrier to entry for adversaries and providing greater confidence and a level of assurance against cyber-enabled attack
- are novel and applicable across a whole "class" of attack surface rather than solutions tailored to a specific threat

[Read the full competition document](#) for more on what technologies we are looking for

Key challenges

DASA is seeking proposals that are applicable across a whole "class" of attack.

We are not seeking solutions that:

- offer demonstrations of off-the-shelf products requiring no experimental development (unless applied in a novel way to the challenge)
- offer no real prospect of integration into defence and security capabilities
- offer no real prospect of out-competing existing technological solutions

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 [Autonomous Cyber Defence for Military Systems](#). This IFA seeks proposals that will develop autonomous cyber defence agents to protect military networks and systems.

[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.

[New consultation for Norfolk habitat restoration project](#)

Press release

A consultation proposal to grant a permit for temporary fish barriers at the entrance to Hoveton Great Broad, Norfolk, is being launched today.

The barriers would form part of a Natural England-led project. The project aims to restore Hoveton Great Broad and Hudson's Bay to a clear water, wildlife rich state by using natural restoration techniques.

The Environment Agency has launched a 'minded-to' public consultation today (16 August) on a flood risk activity permit application from Natural England. This permit is required to allow the installation of the permeable fish barriers.

Earlier this year, a public consultation was held to gather views on the permit application. All responses and application documents were considered and now the Environment Agency has reached a 'minded-to' decision to grant the permit.

An Environment Agency spokesperson said:

> This minded-to consultation gives people the opportunity to view and provide any final comments on the draft permit and draft decision document.
>
> We are keen to hear from anyone who wants to have their say on this proposal before we complete our final decision.

The project proposes to remove the majority of fish from the broad – a technique known as biomanipulation – which will allow water fleas to thrive. These water fleas would then feed on the algae, thereby cleaning the water.

The barriers would be in place for up to 10 years, preventing fish from entering the Broad while the ecology recovers. Once the barriers are removed, the fish will be able to access the restored broad once again.

Responses to the 'minded-to' consultation must be received by the Environment Agency by midnight on 13 September 2021.

Published 16 August 2021
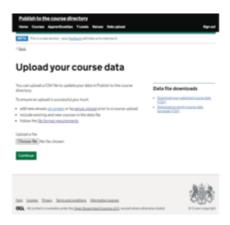Last updated 16 August 2021 [+ show all updates](#)

1. 16 August 2021

   First published.

[New data upload facility on 'Publish to the course directory'](#)

News story

After feedback from users, the National Careers Service has made it easier to upload and update large amounts on information on the platform

The National Careers Service has listened to feedback from providers and introduced a brand-new feature that makes it simpler to upload and update large amounts of information on the 'Publish to the course directory' platform.

The new data upload facility enables providers to import course, apprenticeship and venue data more easily, and presents a great opportunity for providers to review their information and ensure it is as accurate as possible for potential learners to access.

The benefits of the new feature include:

- a simple, step-by-step procedure that tells you where you are in the process.
- provides feedback on the success of the import, and clearly explains where errors exist and how these can be resolved.
- enables users to make corrections online during the upload process.
- greater capacity to upload more information in one go.

To showcase the feature in action, the National Careers Service will be delivering a series of instructional webinars to demonstrate how it works and take users through the process to enable providers to make use of the new data upload feature.

To sign up, simply follow one of the appropriate links below:

[Statement by Nicholas Woolley on the 2021 Zambia election results](#)

World news story

Statement by the British High Commissioner to the Republic of Zambia, His Excellency Mr Nicholas Woolley, congratulating President-elect Hakainde Hichilema.

I offer my warm congratulations to President-elect Hakainde Hichilema for his victory in Zambia's presidential election.

Over the last few days, Zambia has demonstrated the strength of its democratic tradition and can consider itself an example for all nations. Every Zambian, whatever their political persuasion, can take pride in this historic moment.

I applaud the Zambian people for their commitment, resilience and

patience during the election period and all those hard-working staff and volunteers engaged in running such a well-managed and professional electoral process. And I welcome the role of Zambia's political leaders including President Edgar Lungu as the country once again prepares to deliver a peaceful democratic transition.

Zambia and the UK have a broad and deep friendship. The UK Government looks forward to supporting President-elect Hichilema and his Government on their priorities and working on our shared goals in areas such as mutual prosperity, global health security and climate change. We look forward to partnering Zambia in playing a positive role within the region and on the global stage.

Lives have tragically been lost in these elections. We offer our condolences to the victims' families and to all those who have been impacted by violence or abuse in recent months. As with any electoral process, there are divisions that will take time to heal. Now is the moment for magnanimity and reconciliation, to respect the rights of all Zambians to live and prosper together in peace.

Every Zambian has a role to play in uniting and taking their nation forward in the spirit of late President Kenneth Kaunda's legacy — "One Zambia, One Nation".

Published 16 August 2021