HMGCC Co-Creation

Challenge: Novel counter drone and ground station solutions

Summary of the challenge

Counter drone technology is evolving rapidly. As drone threats develop, countermeasures adapt in response, creating a continuous cycle of innovation.

HMGCC Co-Creation is launching a challenge in collaboration with jHub, the central innovation hub for UK Defence's Cyber & Specialist Operations Command, and the Ministry of Justice (MoJ).

This challenge has two distinct, but related workstreams. Solution providers are invited to apply for workstream one, two, or both.

One: jHub require detection and disruption of drone ground control stations, which could be controlling single or swarms of enemy drones.

Two: MoJ need to detect drones commanded over cellular networks via in-built SIM cards in a civilian scenario.

HMGCC Co-Creation will provide funding for time, materials, overheads and other indirect expenses for successful applicants.

Technology themes

Aerospace, data science and engineering, electronic engineering, machine learning, physical security, radio frequency science and engineering, radio systems, robotic and autonomous systems, systems engineering, uncrewed aerial systems.

Key information

Budget per single organisation, up to (ex VAT)	**Workstream one: £60,000** **Workstream two: £60,000**
Project duration	**12 weeks**
Competition opens	**Monday 3 November 2025**
Competition closes	**Thursday 4 December 2025**

Context of the challenge

The threat from drones is frequently seen in the media, as adversaries continue to leverage this technology to do the UK and its allies harm and conduct criminal activity.

jHub – workstream one

The mission of jHub is to bridge the gap between emerging technology and operational requirements, giving defence users the tools to stay faster, smarter, and stronger in a constantly evolving environment.

In modern warzones, various drone technologies are used. From those controlled over radio frequency (RF), cellular networks and fibre optic cables, with low-cost disposable commercial drones to more sophisticated and hardened military grade systems.

While disrupting drones in military operations is achievable, targeting the ground control station where operators pilot these systems could provide significant strategic advantages by reducing adversaries' capabilities.

MoJ – workstream two

The Ministry of Justice is a major government department, at the heart of the justice system, working to protect and advance the principles of justice.

From April 2024 to March 2025 there was a reported 1,712 UAS incidents reported at prisons over England and Wales (https://www.gov.uk/government/news/counter-drone-efforts-rise-as-prison-sightings-revealed). His Majesty's Prison and Probation Service (HMPPS) continually adopts new methods and tools to reduce the risk of such events, but constant innovation is required.

The commercial market is growing for cellular network-controlled drones that use 4G or 5G data connections. This technology allows operators to control drones from any location, even when the drone is beyond their visual range. However, these cellular-controlled drones require different detection methods compared to traditional RF-controlled drones.

The gap

jHub – workstream one

Ground control stations are essential for all drone operations, regardless of the diverse drone technology used in modern conflicts.

Enemy drones on the battlefield are often controlled from positions far behind enemy lines - sometimes up to 40 kilometres away. This distance makes it challenging to locate the control stations, especially given the hostile electronic warfare environment and the use of rebroadcasting stations extending drone range beyond direct line of sight, whilst hiding the true location of the control station.

This challenge focuses on developing technology that can detect and pinpoint the location of enemy ground control stations using information from drones whilst they are in flight. The goal is to then disable all drones controlled by those stations.

MoJ – workstream two

The running of prisons in the UK is complex. HMPPS operates around the clock across urban and rural locations, with any UAS incursions occurring at speed and countermeasures that must comply with UK legal requirements.

There are several counter-drone technologies on the commercial market, but these are typically focused on detection and countering RF controlled drones.

The focus of this challenge lies in semi-automated detection of drones that use cellular networks for control.

Example use case

jHub – workstream one

Captain Jones is commanding a squadron tasked with disrupting drone threats. They are effective at preventing drones causing damage, but this is tackled on a system-by-system basis. To prevent further attacks, he wants to stop these waves at-source.

During a live operational scenario, a swarm of drones is spotted several kilometres away. With numerous drones in the air each day, the first stage is to determine if they are friend or foe.

Captain Jones uses capability that firstly detects and finds more information about the swarm. He discovers it is a mixture of commercial and military grade technology, controlled over an RF link. Captain Jones' equipment then aids him in looking for a way to get information about the Ground Control Station, a vulnerability is found which provides Captain Jones with valuable information.

The technology has a simple user interface, showing the incoming drones overlayed onto maps and displaying a link back to a rebroadcasting station 5 kilometres away from their location, this subsequently shows a link back to another location. This is a strong indicator that this is the ground control station.

The capability would ideally not give away Captain Jones' location. It is also ruggedised and simple to use, perfect for high stress situations.

Captain Jones is deciding what to do next, in the future he may consider taking action himself, but in this situation, he hands the information to his higher command who will take action with different capabilities.

MoJ – workstream two

Charlotte is an officer in a high security prison in an urban location. Over the last year the prison has managed to prevent most drone drops. However, innovation and the demand for illicit items has led prisoners to develop new methods to bypass the prison's existing security measures.

The latest technique involves using commercially available drones that are controlled via cellular networks rather than traditional radio controllers. To counter the new threat, Charlotte is provided with advanced detection equipment.

This new system provides early warning when network-controlled drones approach the prison. The detector can identify active mobile phone connections and distinguish between SIM cards installed in drones and those in regular mobile devices on the network. This device is deployed across the prison service and so must work in a variety of environments.

The detector offers partial automation, flagging to authorities that a drone is in-bound, allowing Charlotte to focus on her core duties. As a result of new tech, proactive steps are taken, and illicit item drops are prevented.

Project scope

In the rapid world of innovation of counter drones, the sponsors require innovative solutions that can be deployed in short timeframes. This means that applicants should aim to deliver physical concept demonstrators within this 12-week project to a Technology Readiness Levels (TRL) of 5 – 9.

It is recommended that proposals label both the existing TRL and the TRL expected by the end of the 12 weeks.

Critical, essential and desirable requirements are listed for each workstream, along with constraints and what is not required.

jHub – workstream one

Critical requirement:

- Detection, identification friend or foe of commercial drones.
- Geolocation of ground control stations to as close-a-position as possible
- Documentation of the proposed solution architecture.
- Documentation of the solution feasibility.

Essential requirements:

- Works for RF controlled drones.
- Shows links between rebroadcasting station and ground control stations.
- Final deliverable is a concept demonstrator handed over to the sponsors.
- Provide full design specifications at end of project.
- Must provide an easy-to-use interface.
- Must be simple to use.

Desirable requirements:

- Works for drones controlled by other means than RF.
- Would ideally not provide a signal that could be located by adversaries.
- Aim for low size, weight and power.
- Ruggedised equipment.
- Detection, identification friend or foe of military-grade UAS.

Constraints:

- Must work in electronic warfare environments.

Not required:

- Horizon scanning only.

MoJ – workstream two

Critical requirement:

- Detection of cellular network-controlled drones.
- Must minimise interference and invasion of other non-targeted electronic signals.

Essential requirements:

- Final deliverable is a concept demonstrator handed over to the sponsors.
- Provide full design specifications at end of project.
- Must provide an easy-to-use interface.
- Must be simple to use.
- Provide an early warning, tracking position and flight path of drones.

Desirable requirements:

- Provides automated detection with minimal user input required.
- Aim for low size, weight and power.
- Ruggedised equipment.
- Minimise false positive alerts from other devices on the cellular network.
- Adaptable as new cellular frequencies are used.
- Portable and usable across numerous site locations.

Constraints:

- Must operate within legal frameworks.
- Prefer to not require information directly from telecommunication operators.

Not required:

- Horizon scanning only.
- Detection of RF or fibre-optic controlled drones.

Dates

Competition opens	Monday 3 November 2025
Clarifying questions deadline	Tuesday 18 November 2025
Briefing Call (Please note: Recording or use of AI notetakers is not permitted)	Tuesday 18 November 2025 at 11am
Clarifying questions published	Tuesday 25 November 2025
Competition closes	Thursday 4 December 2025
Applicant notified	Monday 22 December 2025
Pitch day (1) in Milton Keynes	Tuesday 6 January 2026
Pitch day (2) in Milton Keynes	Wednesday 7 January 2026
Pitch Day outcome	Wednesday 14 January 2026
Commercial onboarding begins*	Tuesday 20 January 2026
Target project kick-off	Early February 2026

*Please note, the successful solution provider will be expected to have availability for a one-hour onboarding call via MS Teams on the date specified to begin the onboarding/contractual process.

Eligibility

This challenge is open to sole innovators, industry, academic and research organisations of all types and sizes. There is no requirement for security clearances.

Solution providers or direct collaboration from countries listed by the UK government under trade sanctions and/or arms embargoes, are not eligible for HMGCC Co-Creation challenges.

How we evaluate

All proposals, regardless of the application route, will be assessed by the HMGCC Co-Creation team. Proposals will be scored 1-5 on the following criteria:

Scope	Does the proposal fit within the challenge scope, taking into consideration cost and benefit?
Innovation	Is the technical solution credible, will it create new knowledge and IP, or use existing IP?
Deliverables	Will the proposal deliver a full or partial solution, if a partial solution, are there collaborations identified?
Timescale	Will the proposal deliver a minimum viable product within the project duration?
Budget	Are the project finances within the competition scope?
Team	Are the organisation / delivery team credible in this technical area?

Invitation to present

Successful applicants will be invited to a pitch day, giving them a chance to meet the HMGCC Co-Creation team and pitch the proposal during a 20-minute presentation, followed by questions.

After the pitch day, a final funding decision will be made. For unsuccessful applicants, feedback will be given in a timely manner.

Clarifying questions

Clarifying questions or general requests for assistance can be submitted directly to cocreation@hmgcc.gov.uk before the deadline with the challenge title as the subject. These clarifying questions may be technical, procedural, or commercial in subject, or anything else where assistance is required. Please note that answered questions will be published to facilitate a fair and open competition.

How to apply

Please submit your application on the HMGCC Co-Creation website. Any queries please email Co-Creation@dstl.gov.uk and cocreation@hmgcc.gov.uk.

All information you provide to us as part of your proposal will be handled in confidence.

Applications **must** be no more than six pages or six slides in length. HMGCC Co-Creation reserve the right to stop reading after 6 pages if this limit is breached. The page/slide limit excludes title pages, references, personnel CVs and organisational profiles.

There is no prescribed application format, however, please ensure your application includes the following:

Applicant details	Contact name, organisation details and registration number.
Scope	Describe how the project aligns to the challenge scope.
Innovation	Describe the innovation and technology intended to be delivered in the project, along with new IP that will be generated or existing IP that can be used.
Deliverables	Describe the project outcomes and their impacts.
Timescale	Detail how a minimum viable product will be achieved within the project duration.
Budget	Provide project finances against deliverables within the project duration.
Team	Key personnel CVs and expertise, organisational profile if applicable.

Co-Creation terms and conditions

Proposals must be compliant with the HMGCC Co-Creation terms and conditions; by submitting your proposal you are confirming your organisation's unqualified acceptance of Co-Creation terms and conditions.

Commercial contracts and funding of successful applications will be engaged via our commercial collaborator, Cranfield University.

HMGCC Co-Creation supporting information

HMGCC works with the national security community, UK government, academia, private sector partners and international allies to bring engineering ingenuity to the national security mission, creating tools and technologies that drive us ahead and help to protect the nation.

HMGCC Co-Creation is a partnership between HMGCC and Dstl (Defence Science and Technology Laboratory), created to deliver a new, bold and innovative way of working with the wider UK science and technology community. We bring together the best in class across industry, academia, and government, to work collaboratively on national security engineering challenges and accelerate innovation.

HMGCC Co-Creation aims to work collaboratively with the successful solution providers by utilising in-house delivery managers working Agile by default. This process will involve access to HMGCC Co-Creation's technical expertise and facilities to bring a product to market more effectively than traditional customer-supplier relationships.

FAQs

1. **Who owns the intellectual property?**

   As per the HMGCC Co-Creation terms and conditions, project IP shall belong exclusively to the solution provider, granting the Authority a non-exclusive, royalty free licence.

2. **Who are the end customers?**

   National security users include a wide range of different UK government departments which varies from challenge to challenge. This is a modest market and so we would encourage solution providers to consider dual use and commercial exploitation.

3. **What funding is eligible?**

This is not grant funding, so HMGCC Co-Creation funds all time, materials, overheads and indirect costs.

4. **How many projects are funded for each challenge?**

On average we fund two solution providers per challenge, but it does come down to the merit and strength of the received proposals.

5. **Do you expect to get a full product by the end of the funding?**

It changes from challenge to challenge, but it's unlikely. We typically see this initial funding as a feasibility or prototyping activity.

6. **Is there the possibility for follow-on funding beyond project timescale?**

Yes it is possible, if the solution delivered by the end of the project is judged by the HMGCC Co-Creation team as feasible, viable and desirable, then phase 2 funding may be made available.

7. **Can we collaborate with other organisations to form a consortium?**

Yes, in fact this is encouraged, and additional funding may be made available. Please see the maximum budget of the individual challenge.

8. **I can't attend the online briefing event, can I still access this?**

If a briefing event is held, any questions (and answers) will be captured and published after the event. The call itself is not recorded and use of AI notetakers is not permitted.

9. **Do we need security clearances to work with HMGCC Co-Creation?**

Our preference is work to be conducted at OFFICIAL, we may however, request the project team undertake BPSS checks or equivalent.

10. **We think we have already solved this challenge, can we still apply?**

That would be welcomed. If your product fits our needs, then we would like to hear about it.

11. **Can you explain the Technology Readiness Level (TRL)?**

Please see the UKRI definition for further detail.

12. **Can I source components from the list of restricted countries, e.g. electronic components?**

Yes, that is acceptable under phase 1 - feasibility, as long as it doesn't break UK government trade restrictions and/or arms embargoes.

Further considerations

Solution providers should also consider their business development and supply chains are in-line with the National Security and Investment Act and the National Protective Security Authority's (NPSA) and National Cyber Security Centre's (NCSC) Trusted Research and Secure Innovation guidance. NPSA and NCSC's Secure Innovation Action Plan provides businesses with bespoke guidance on how to protect their business from security threats, and NPSA and NCSC's Core Security Measures for Early-Stage Technology Businesses provides a list of suggested protective security measures aimed at helping early-stage technology businesses protect their intellectual property, information, and data.