CySpace Connected Capability Network

UK-CYSPACE

Powered by Satellite Applications Catapult

CATAPULT Satellite Applications

Formatting by:

CGI

CySpace Connected Capability Network (CCN)

A path to secure and resilient growth in the UK Space Sector

Overview

The UK's growing reliance on space-based infrastructure—satellite communications, positioning, navigation and timing (PNT)—creates a critical national vulnerability. Threats to these systems are increasing in frequency, sophistication, and impact, spanning cyber, electromagnetic and physical domains.[1]

Recent incidents, including the 2022 ViaSat[2] attack, demonstrate how disruption to space systems can cascade across critical sectors including energy, transport, telecommunications and finance. The resilience of the UK space domain is therefore a matter of national security and economic stability.

This paper sets out a clear, evidence-based roadmap to strengthen UK space-cyber resilience. Drawing on engagement with over 250 experts across government, industry, academia and defence, it identifies three systemic challenges:

- Fragmentation across governance, communication and capability
- Insufficient coordination and funding of academic research
- Limited awareness of the threat landscape, particularly among SMEs

To address these challenges, CySpace CCN proposes three targeted, deliverable recommendations designed to improve coordination, capability and national resilience at pace.

[1] Space-ISAC_Q1-2025-Public-Report_TLP-CLEAR-1.pdf

[2] Case Study: Viasat Attack | CyberPeace Institute

The case for action

The UK space sector operates within a complex, fragmented landscape involving multiple government departments and agencies, including MoD, DSIT, DfT, FCDO, UKSA, CAA, NCSC and NPSA. While each plays a critical role, the absence of a unified approach to space cyber security creates:

- Barriers to effective information sharing
- Inconsistent standards and expectations
- Limited visibility of threats and available support

At the same time, the sector is dominated by SMEs, many of which lack the capacity to prioritise cybersecurity without clearer guidance, incentives and support. Furthermore, theability to coordinate and effectively support clear and coherent security frameworks creates barriers to export and growth in the sector. Without coordinated intervention, these gaps will continue to increase systemic risk across the UK economy.

The CySpace CCN

The CySpace CCN is one of four CCNs, established in 2024 is a UK wide network led by the Space West space cluster funded and supported by Satellite Applications Catapult, a government funded organisation focused on growing the space sector. The aim of CySpace is to create a more resilient space domain by bringing together representatives from industry, academia and government within and outside the space sector, taking a structured approach to mapping relevant capabilities and expertise that can be leveraged to address critical vulnerabilities. Based on advice and guidance from industry and government the initial focus of CySpace was on securing Space Domain Awareness (SDA) in the UK against cyber attacks.

SDA includes characterisation, attack attribution, threat modelling, capability and behavioural analysis as described in Ministry of Defence Joint Doctrine Publication 0-40. The working group looked at the collection, sharing, processing and analysing of electronic data for the purposes of supporting the tasks outlined above. SDA provides the data and information needed to operate safely, securely and sustainably in space, and is central to UK Space Command's Protect and Defend mission. Discussions about SDA and cyber security revealed problems with the broader space and cyber security mission. CySpace provides a forum for experts to share their knowledge, identify socio-technical gaps in the UK's ability to protect and defend space infrastructure, and work collaboratively to develop recommendations and a roadmap for CySpace to contribute towards a more connected and secure space sector.

Through a structured programme of:

- A cross-sector Working Group, 25 experts from industry, academia and government
- A formal Requirements Catalogue[3] aligned to the NCSC Cyber Assessment Framework
- Six regional workshops engaging 200+ professionals

CySpace has mapped both the threat landscape and UK capability, identifying strengths but also systemic weaknesses that require coordinated national action.

CySpace used this structure approach to map UK capability against those outlined in the Requirements Catalogue through six regional workshops, engaging with over 200 cyber security and space professionals from across the UK. This exercise revealed exceptional regional capabilities in cyber security that addressed many areas identified within the Requirements Catalogue. Beyond this, the workshops exposed a far broader fundamental set of problems that exist in securing space systems and developing solutions that have been set out in the CySpace Problem Book[4] which has been summarised in Annex B. This work has revealed a broader purpose for the CySpace programme, to help solve fundamental problems across cyber and space domains within the UK.

[3] CySpace CCN Requirements Catalogue

[4] CySpace CCN Problem Book

Critical challenges

The Working Group reconvened in late 2025, to prioritise the most important problems and gaps to create a set of recommendations for CySpace to work with the ecosystem to deliver:

Fragmentation

Whilst much work has been done to build towards a 'One Government' approach to space, the sector remains incredibly fragmented and challenging to navigate, especially with respect to cybersecurity.

According to the UKSA 'Space operations and their security involve multiple government entities including the Ministry of Defence (MoD), Foreign, Commonwealth & Development Office (FCDO), Department for Transport (DfT), and Department of Science, Innovation and Technology (DSIT).'

There is no trusted point of contact for space and cyber problems, either across or within the two industries. This fragmentation creates multiple problems and makes it harder to surface, correlate and act on weak signals, incidents and lessons learned. There are multiple forums where space and cyber are discussed, but not all are open to everyone, and it is unclear if and how information sharing is happening between these groups. The result is that cyber security within the space sector is not understood or implemented as fully as it needs to be, and there are barriers to getting out a full, clear and consistent message.

Academic research

Whilst there is a wealth of expertise in academia across both cyber and space, academic research is often conducted in silos. Furthermore, the division of responsibility between UK research councils for space and cyber security between STFC and EPSRC has led to a dearth of funding for space specific cybersecurity research which is critically important given the unique non-terrestrial constraints that space security involves. Alongside this there are limited academic networks in this area making it challenging for the community to collaborate and share findings.

Limited threat awareness

Awareness of space-cyber risks remains uneven, particularly outside government and defence. Stakeholder engagement identified some systemic issues which are considered responsible

- The UK's space sector is dominated by SMEs- of the 1,765 organisations operating within the space sector in the UK approximately 1,600 are SME and account for only 10% of the sector income. These critical factors mean that they often lack capacity and resources to understand threats and prioritise cybersecurity
- Existing government support is underutilised – UK Space Agency, NCSC, CAA, NPSA have funding, resources and support available through their individual organisations yet coordination and communication of available support is poor with visibility and ability to navigate for new entrants challenging

Information is fragmented across multiple organisations – given the split of responsibility for security in the space sector information on threats is challenging to access and not available to smaller organisations This results in underinvestment in security and increased systemic vulnerability.

Recommendations

Recognising the need for better coordination, cohesion and communication across the space and cyber sectors, that enables industry, academia and government to understand, innovate and act, the CySpace Working Group proposed three recommendations that will deliver the highest impact. These will be taken as a roadmap of future work upon which to further our long-term ambition and progress in a way that complements existing UK institutions and relevant Space ISAC activity. The aim of CySpace is not to replicate the good work that is already being done. Our goal is to act as the facilitator and coordinator of existing initiatives.

Single source of coordination and trusted threat-sharing for space security issues – A UK Global ISAC Watch Centre

Establish a trusted, industry-led, government supported national focal point to act as the single interface for space cyber security, reducing fragmentation across government, industry and academia. This function should align with existing UK institutions and integrate with the Space ISAC and its UK Global Hub, enabling access to international threat intelligence, shared processes and trusted networks.

Over time, this capability should evolve into a UK Space ISAC Watch Centre, able to receive and sanitise incident data, enable anonymised sharing under the Traffic Light Protocol (TLP), and issue UK-specific advisories and playbooks. It should maintain clear links with NCSC, UKSA, UK Space Command and regulators, while leveraging regional space clusters to ensure nationwide engagement.

This capability would strengthen the resilience of the commercial space sector, enhance the UK's Space Domain Awareness, and improve access to global threat intelligence. It would also support innovation by creating clearer pathways for security products and services.

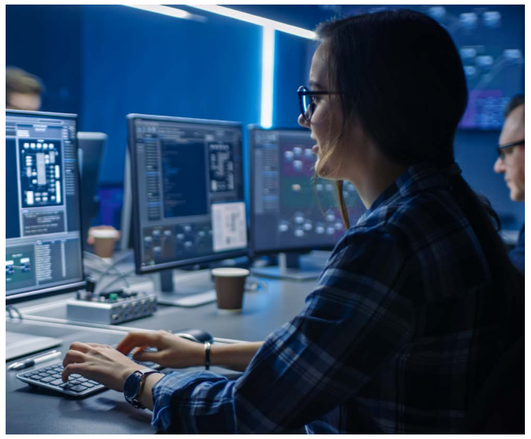
Space Information Sharing and Analysis Centre (ISAC)

The Space ISAC is a US based, industry led centre that facilitates collaboration across the global space industry to enhance the ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information.

Whilst Space ISAC was first established in the US, it is leading the expansion of a global ISAC community, developing watch centres across allied nations with the global hubs being established in Australia, UK, Canada and Japan to deliver 24-7 information sharing.

Catalogue of available support

We recommend the creation of a catalogue of available support to be available in one single point on a website, to mitigate lack of visibility for space and cyber resources. This could be championed through the regional space clusters, and act as a starting point for identifying suitable resources for securing space companies. The catalogue should include the resources available and key cyber and space requirements, opportunities and funding. It should provide enhanced guidance to companies and should be linked to the focal point above so that static guidance is complemented by current alerts, reporting routes, points of contact and relevant Space ISAC and UK resources. This could build upon UKSA's existing one stop shop for information.



Facilitating academic research and collaboration

CySpace recommends the creation of a new interdisciplinary cyber and space research network developing interaction between the research community and appropriate science, technology and industrial groups. The network could target EPSRC network grant funding and would facilitate

- the transfer of knowledge, model and insights into industry and government,
- provide insight into emerging technologies and associated risks
- promote mobility between academia, universities and industry
- generate new multidisciplinary research proposals, centres of excellence and a critical mass of expertise
- influence the flow of funding available for space specific cyber security research

The network should also maintain a structured link to operational communities, including relevant Space ISAC Working Groups, relevant Watch Center outputs and international partners. This way, UK research priorities reflect live threat trends and mission needs.

Cyspace 2.0

CySpace recognises that space cyber security is a continuous, evolving challenge requiring sustained coordination as new entrants and technologies emerge. As CySpace moves forwards it will continue to maintain its role as a national convenor, strengthening collaboration and supporting a more resilient, connected and secure UK space sector by:

- Assessing the funding and resource requirements needed to deliver the proposed initiatives
- Supporting the long-term ambition of establishing a central UK hub for space and cyber security, connecting government, military, industry and academia.
- Enable stakeholders to develop and implement the infrastructure outlined in the recommendations.
- Build on existing Space ISAC practices and established UK partnerships where appropriate.

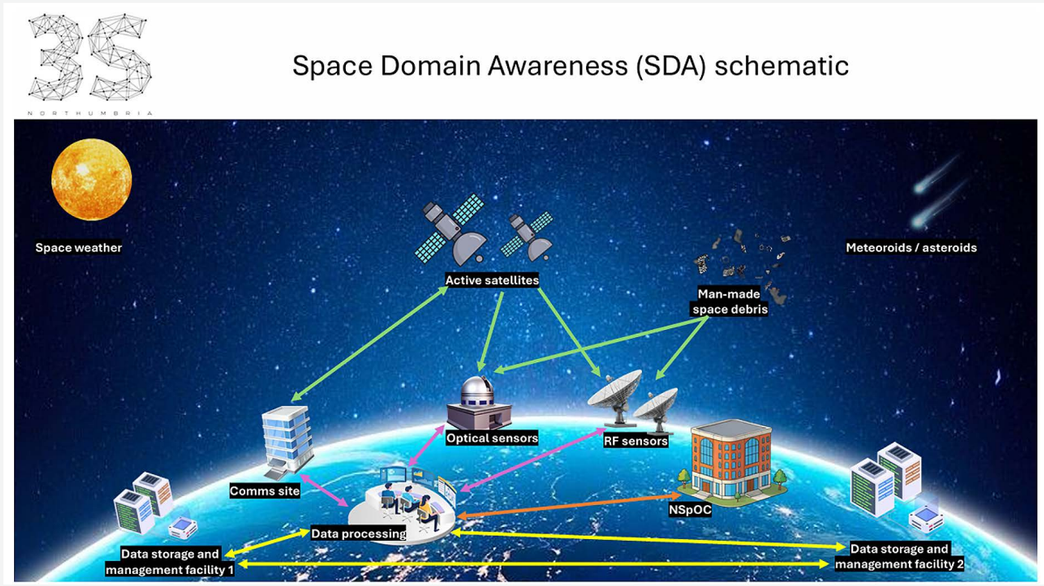
Signed:

We would like to thank CGI for support with formatting this report.

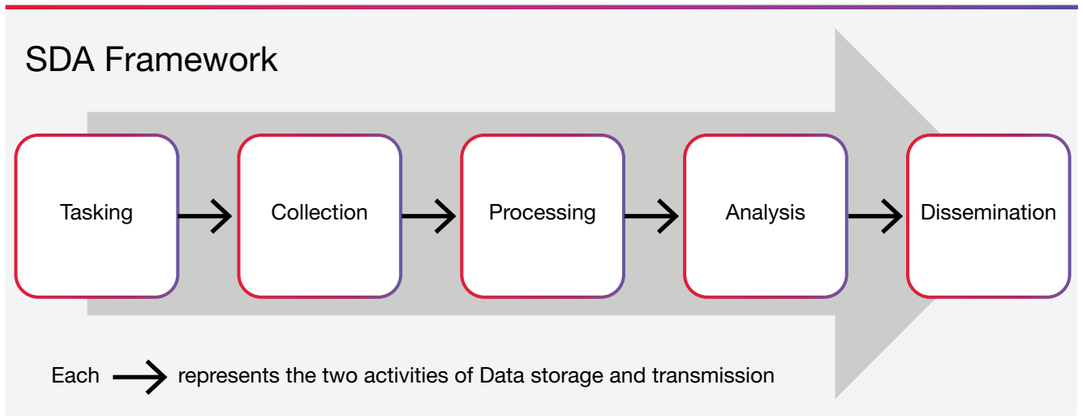
Annex

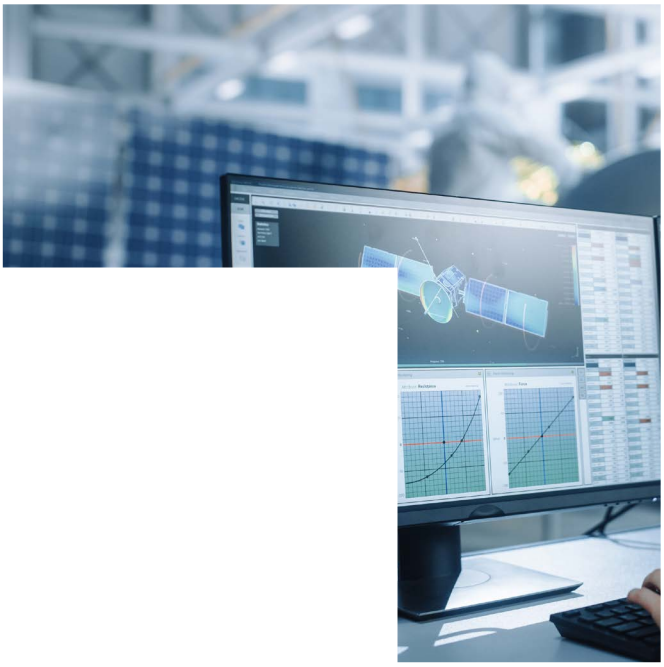
Annex A

i. Architecture model of space domain awareness, developed by Kseniia Hryshchuk, 3S Northumbia and from CySpace Working Group discussions co-led by Frazer Nash Consultancy.



ii. Architecture model to describe the storage and transmission of data through the space domain awareness process.





About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. We are insights-driven and outcomes-focused to help accelerate returns on your investments.

For more information about CGI, visit:
cgi.com/uk/space
or email us at enquiry.UK@cgi.com