UK-CYSPACE

CySpace CCN – Summary of Cyber Security and Space Domain Awareness Capability Mapping Workshops and Problem Book

Background

The domain of space is becoming increasingly congested, contested and competed as space actors, state and private enterprise, seek to reap the benefits space systems can provide. As innovation continues to broaden the capabilities of space systems, these are playing an increasing role in facilitating functions of society, economy and national security. Space is identified as part of our Critical National Infrastructure and strengthening the security of our space assets must be a priority for the sector and government to ensure our social and economic prosperity.

The CySpace Connected Capability Network aims to create a more resilient space domain by bringing together partners from across industry, academia and government within and outside the space sector to map relevant capabilities and expertise that can be leveraged to create new products and services that address our most critical vulnerabilities.

This summary pack covers the workshops held in work package two which were used to compile a map of UK's current capabilities in cyber security for space. This followed on from the requirements definition stage of the project, and the information acquired will support the generation of a gap analysis and development of a roadmap.

This document is for everyone within the CySpace network across the UK to have visibility of the outputs from the workshops. The CySpace team are open to any feedback from industry, academia and government perspectives on the problems and suggestions highlighted.

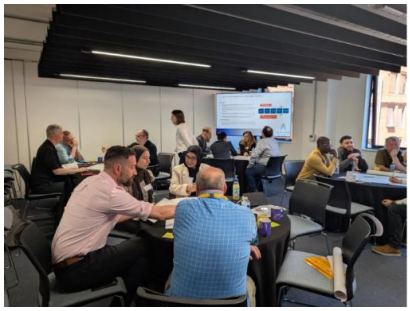
Description

This document contains a summary of the problems and solutions which emerged within the workshops, categorised by each Requirement Catalogue Theme, as well as a summary of each workshop.

Workshops Summary

A total of 6 workshops were delivered across the UK, with a focus on discussing, collecting and collating a detailed understanding of the UK's capabilities in cyber security for space. These events were attended by a wide range of organisations from across industry, academia and government.

North West: DiSH, Manchester, 9th May, 10am-4pm



The NW workshop in Manchester was the first one delivered, and therefore our first opportunity to reach out to regional space and cyber communities. There was a lot of enthusiasm in the room for tackling the perceived challenges of securing space domain awareness and developing infrastructure to support a formal response to them. As a result of the discussions within this workshop, a collaboration has emerged to develop Northwest physical space and cyber security infrastructure.

Northern Ireland: The Centre for Secure Information Technologies, Belfast, Queen's University Belfast, 3rd June 10am-4pm

This workshop revealed interesting niches within the SDA and cyber disciplines, and many relevant capabilities, including academic courses focused on AI and computer science – demonstrating the potential benefits of more collaboration across the UK. The workshop itself was quite academically focused in terms of participants, and this potentially influenced the outcomes of studies. The NI region benefits from both NI infrastructure and UK wide infrastructure, with NCSC mentioned briefly, but there are clear gaps in communication between the NI region and UK government. As a result of the enthusiasm in this workshop, CySpace was invited to present a talk at the event "Cyber Security in Defence" on 23rd October 2025 at NIACE Belfast.

UK-CYSPACE

South West: The Bottle of Sauce, Cheltenham, 5th June, 11am-5pm

The SW workshop had a lot of industry presence, as well as some from academia and government. The discussions were often focused on the practicality of cyber security for space, and how it fits with industry priorities. This workshop concluded on a more cautious note to further discover how solutions to securing SDA can be sensible and realistic for industry.

North East: Stephenson Building, University of Newcastle, Newcastle, 26th June, 10am-4pm

The NE workshop took place in Durham. This was a smaller scale workshop, but there was lots of expertise about SDA and space situational awareness in the room. In this region, there is convergence between space and cyber through the space cluster and cyber cluster, and this was reflected in discussions and an appreciation for collaboration between the two industries. As a result of this workshop, CySpace was invited to further support the North East space and cyber security eco system, as a panellist at the event "Cyber Security in the Space Economy" on 15th October at Durham Cricket.

Scotland: Edinburgh Climate Change Institute, Edinburgh, 4th September, 10am–4pm

The workshop in Edinburgh was oriented quite heavily around what Scotland has already achieved in terms of setting global precedents in space – for instance Space Sustainability: A Roadmap for Scotland 2022, one of the first roadmaps to be developed for sustainability in space. The attendees were enthusiastic and specialised across multiple fields, including the legal and regulatory aspects of securing space. The outcome was a hopeful closer focus on space and cyber within existing Scottish infrastructure, such as Space Scotland.

UK-CYSPACE

Central South: BaseKX, University College London, London, 23rd September, 10am-4pm.

The final workshop in the series took place in London. For this workshop, we had a lot of industry presence, as well as academia and some government. As a result the discussions were focused on forward thinking methodologies and emerging technology. This was also the largest workshop in terms of in-person attendees, with around 40 attending, and this provided an especially great networking opportunity for space and cyber in the region.

Requirements Catalogue – Problems and Suggestions

The workshops resulted in a list of common problems and suggested solutions for improving support of cyber security for space domain awareness in the UK, associated with each theme within the Requirements Catalogue, as provided below:

Managing Security Risk Governance including risk, asset, comms and data management, and supply chain analysis for physical and data assets.

Problems

- **Geopolitics** Within the area of managing security risk governance, geopolitics emerged multiple times as a key problem, in terms of whether the standards in each country meet the need for secure systems. Also, as global tensions rise, countries are relying on allies for redundancy and backups of their space systems.
- **Evolving Risks** Another problem is that risks evolve rapidly, and standards do not always keep up with these changes. For instance, considering the pace of new technology such as AI and quantum and the perceived inability for standards authorities to keep up with innovation.
- **Fragmentation** A further problem is the fragmentation of space infrastructure in the UK, as reflected in the lack of communication between government and industry, wide ranging standards for securing space and clarity on roles and responsibilities in case of an attack to critical space systems. Governments feel distant and companies do not know who to contact about risks to space systems.
- **Innovation** In addition, there is a balance between corporate success and social responsibility, also with implications for nurturing innovation in the space domain.
- **Information Sharing** And finally, a lack of information sharing was highlighted, to include knowledge exchange and lessons learned.

Suggestions

- **Data availability** Development of data sharing mechanisms would make more data available about threats to space systems. This could involve open data sharing and commercialisation of data.
- **Unique Selling Points** Another suggestion is to clarify each region's unique selling point, including capabilities. This should be a community-led approach to identify each region's priorities, competitions and scalable assets, with the benefits of improving each region's competitiveness and boosting regional collaboration.
- **Infrastructure** Other solutions suggest the development of more infrastructure to support research and testing cyber security and space domain awareness. This may involve taking advantage of expertise in academia, for instance for universities to develop data analytic skills. This may also look like a cyber security intelligence lab for testing in a secure site with secure suppliers and software.
- **Roadmap** A final suggestion was to develop a roadmap involving space "champions" who can highlight opportunities in the sector, provide advisory to government with benefits of clarity of standards surrounding securing space.

Protecting Against Cyber Attacks including data and system security, data lifecycle and involved actors, resilience through backups and repositories, staff awareness and training and service protection policies, processes and procedures.

Problems

- **Resilience** Cyber compliance is often out of date, and detection of attacks happens too late. It is important to have redundancies for when an attack inevitably targets a system, such as terrestrial backups.
- **AI** Artificial intelligence emerged as a problem too big to manage and govern.
- **Attitudes** There was critique of attitudes towards securing space assets, including those which assume if a system is not broken, it does not need to be fixed. Another attitude is a preconception that security issues are someone else's problem. This is further reinforced by the fact that cyber security is commonly outsourced to an external company – and perhaps not integrated into company ethos.
- **Unique Problems** Some unique problems with securing space assets emerged, to include the remote nature of space assets giving attackers to opportunity to target sensors and reliance on individual organisations to provide space services.

Suggestions

- **Standards** More standards provided by government which are specific to space, implemented by standards agencies which are transparent and maintain a high reputation.
- **Culture** Nurture a culture with a security forward mindset and consistent auditing, to ensure more efficient security of assets.
- **Knowledge Sharing** Sharing insights and approaches to resilience of space systems, such as technology and facilities, opening opportunities for learning from companies across sectors.
- **Risk Governance** Promoting "good" risk governance within the space sector, to include defining the recovery time and point objectives of IT capability aligned to critical processes, alignment of continuity and resilience in cyber strategies.
- **Infrastructure** In order to develop more sovereignty over UK assets, infrastructure should be developed, such as additional observatories in order to improve capabilities in radars and sensing.
- **Skills** Develop skills drawing upon extensive expertise in academia, perhaps through development of a problem book for space and cyber for training and awareness, with advisors from government agencies.

Detecting Cyber Security Events

Security Monitoring, with proactive security event discovery, latency and remote access issues, AI and autonomous defence.

Problems

- **Threat Surface** The convergence of information technology and operational technology is expanding the threat surface. The future threats are also currently not well understood, including how quantum cryptography will change the threat landscape.
- **Resilience** There is not enough focus on resilience in terms of cyber security regulations and also meeting demands of the national skills gap.
- **Threat Landscape** There is not much understanding about how attackers are targeting the space sector. This is worsened as the threat landscape is always changing and modern technology such as AI is adding complexity, as it gives threat actors access to more advanced systems and also the more data is outsourced increases access points.
- **Cyber Regulation** There are insufficient cyber security regulations, and no one wants to own them. This is worsened by extensive supply chains, which are challenging to fully regulate, even with a list of requirements, and rapidly emerging and changing threats.
- **Communication** Teams may have sufficient technical skills to tackle challenges, but they act in siloes and do not communicate with each other enough. This is partially due to a lack of funding for soft skills including communication, and too much emphasis on hard skills.
- **Remote Access** As many systems are remotely operated, attackers can exploit opportunities to execute social engineering attacks including imitating IT companies and asking for password reset.

- **Data** It is challenging to collect data from some space assets, and this makes it difficult to understand what is normal and spot anomalies, as well as what is needed for more sovereignty over space services.
- **Academia** There is a lack of focus on cyber security for space domain awareness in academia, and also not much visibility of those focusing on this niche area.
- **Detecting Threats** There is a lack of monitoring companies in this niche area and detection of threats can be challenging given the global distribution of infrastructure – making physical monitoring and access to data sometimes challenging.
- **Risk Attitude** Business priorities such as reputation and share price take priority in decisions about security. For instance incidents may not be reported due to potential impact on share price.

Suggestions

- **Security Culture** There should be more awareness of the benefits of a positive security culture in terms of cost vs benefit.
- **UK Standard** The UK could develop a focused space regulation from government to cover people, processes and technology, potentially led by the British Standards Institution. This could be an opportunity to upskill space companies and encourage collaboration with the cyber industry. The Civil Aviation Authority could also emphasise support for the best and cheapest technology by providing a cyber security wrapper.
- **Communication and Training** Mass communication about the security of space could help to raise awareness of it and emphasise its importance. Part of this strategy could be to train people in associated skills which do not require a degree, and training for managing emerging technology such as AI. This would also aid understanding of the sector and the need for bespoke solutions.

UK-CYSPACE

Minimising the Impact of Incidents, including response, recovery, lessons learned, resilience through space assets and AI/autonomy solutions.

Problems

- **System Understanding** There is not full understanding of space systems as a whole, including what is needed to secure them and the challenges emerging technology is bringing to the sector. This extends to the supply chain, including data supply chain, and in-orbit services.
- **Authoritative Body** It is challenging to understand who is in charge in space cyber security and also UK specific requirements.
- **Limited Monitoring** There are limited companies focused on monitoring space and physical positioning of space objects, worsened by false datasets and fragmentation of datasets.
- **Data Sovereignty** The electrical supply for data centres is not always sovereign, and this has implications for associated skills development in the UK, with an impact of the UK's data sovereignty.
- **Data Sharing** UK space sector does not share data or do enough desktop exercising, with implications for understanding the whole space system and its threat landscape and also limiting incident response capabilities.
- **Monitoring Threats** There are limited UK companies monitoring threats in space, with impacts on foresight on potential disruption.

Suggestions

- **Training** This should incentivise good behaviour and deepen understanding of space and cyber issues, with learning from other sectors such as finance integrated within. This could be further built upon by valuing space and cyber skills more highly with better pay rates.
- **Cloud Sovereignty** Cloud Act or Safe Harbour Act could be developed, integrating megawatts vs gigawatts, and specifically operating for space, and industry could be responsible for implementing it. This would also bolster national sovereignty and expertise of space services.
- **Information Sharing** Developing a platform to exchange information could help the space sector learn from the finance sector which is driven by regulations and also nurture a forum for sharing recovery approaches. This would also lead to better understanding of risks and threats and help with understanding the cost of not investing in cyber security.
- **Emphasise Resilience** There should be focus on building resilience in space, in terms of adaptability and changing models, and availability of multiple backup systems. This also includes back up hardware, such as ViaSat's replacement modems from 2022 and the use of AI and autonomy to help get communications back online.

General

Additional problems

- Overclassification of information
- Ability for start-ups and SMEs to manage security by design and verify trusted data.
- Geographic relevance can be limiting. For instance, the NI workshop revealed a lack of connection with the rest of the UK, for instance with no UKSA presence in the region.
- Cyber security and SDA are linked with modern technology, such as quantum key distribution and AI – and ask these technologies evolve, they will impact the UK's ability to protect SDA.
- There are many companies which are specific to each region, including academic institutions, although it is unknown how they link together nationally.
- Some large companies, such as Deloitte and Thales have presence across multiple regions in the UK, helping to link capabilities together.
- There is a clear lack of infrastructure for data sharing within the UK, including between academic institutions and industry.

Additional solutions

- Supplier Portals Provide for more visibility on suppliers through formal portals