UK-CYSPACE

FRAZER-NASH
CONSULTANCY
A KBR COMPANY

CySpace Connected Capability Network

Cyber security for space domain awareness requirements catalogue

fnc.co.uk

Background

The CySpace Connected Capability Network (CCN) 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 CySpace CCN is led by Space West and delivered in partnership with Frazer-Nash Consultancy, Space South Central, North West Space Cluster, Space North East, Space Wales, Space East and NI Space as well as the cyber cluster from across the UK. The programme is funded and supported by the Satellite Applications Catapult as part of their Connected Capability programme.

One of the key activities of the programme is to identify the cyber security requirements for Space Domain Awareness (SDA) activities within the UK, map capabilities that already exist, and highlight subsequent gaps. This understanding will then be used to identify and prioritise the required programmes and activities to fill these gaps and create a roadmap for investment.

As part of the programme, a series of work packages have been set up, including work package 1, led by Frazer-Nash. This has seen the establishment of a working group comprising of individuals representing government, military, academia, prime contractors and Small to Medium-size enterprises (SMEs) and the facilitation of four workshops. The purpose of these workshops has been to develop a requirements catalogue covering cyber security for SDA.

This report provides an overview of the discussions that took place, diagrams showing the technical architecture of SDA and the organisations involved in securing it, and the requirements catalogue.

1. Working group

A working group was set up to ensure that the views and experience of relevant stakeholders were taken into consideration. The group was made up of representatives from government, military, industry (both prime contractors and SMEs) and academia.

Composition of working group included

Government/Military:

- UK Space Command
- UK Space Agency

Prime contractors:

- Frazer-Nash Consultancy
- Lockheed Martin
- PA Consulting
- Raytheon
- MBDA

Academia:

- University of Bristol
- University of Durham
- University of Surrey
- Queen’s University Belfast
- University of Lancaster

SMEs:

- Risk Aware
- Actica
- Angoka
- UDSS
- Actica
- Aiion

Workshop topics

The group met over the course of four workshops, exploring the following themes.

Workshop theme of discussion

1. Definitions of SDA and cyber security
2. Threats within SDA
3. Mapping threats to established Cyber Assessment Framework
4. Formation of the requirements catalogue

Discussions in workshop 1 covered the definitions of SDA and cyber security that were to be used, and a framework to explain the breakdown of SDA activities.

To ensure that there is consistency and clarity of understanding for the purposes of this catalogue and programme the working group agreed the following definitions. **The agreed definition for SDA is:** as described in JDP 0-40:

- Space Surveillance and Tracking (SST) – including sensor tasking and management, orbit determination and propagation, catalogue maintenance, launch and manoeuvre detection
- Space Situational Awareness (SSA) – including conjunction and fragmentation analysis, re-entry warning, launch collision avoidance, laser range clearance, space weather warnings, frequency deconfliction, orbital slot station-keeping monitoring
- Space Domain Awareness (SDA) – including characterisation, attack attribution, threat modelling, capability and behavioural analysis.

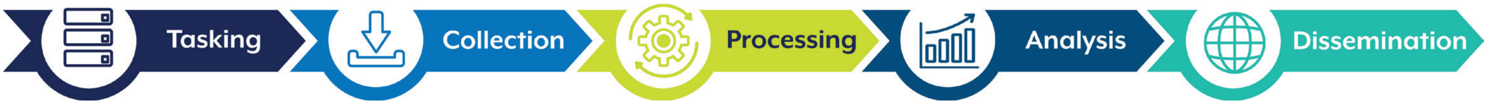
For this project, we are looking at the collection, sharing, processing and analysing of electronic data for the purposes of supporting the tasks outlined above.

The agreed definition for cyber security is:

> “The protection of devices, services and networks - and the information on them – from unauthorised access, theft or damage.”

2. The SDA framework

The SDA Framework describes the main activities within SDA with respect to data, including the movement of data between and across the activities. The diagram below describes this movement. Each arrow represents the two activities of data storage and transmission.



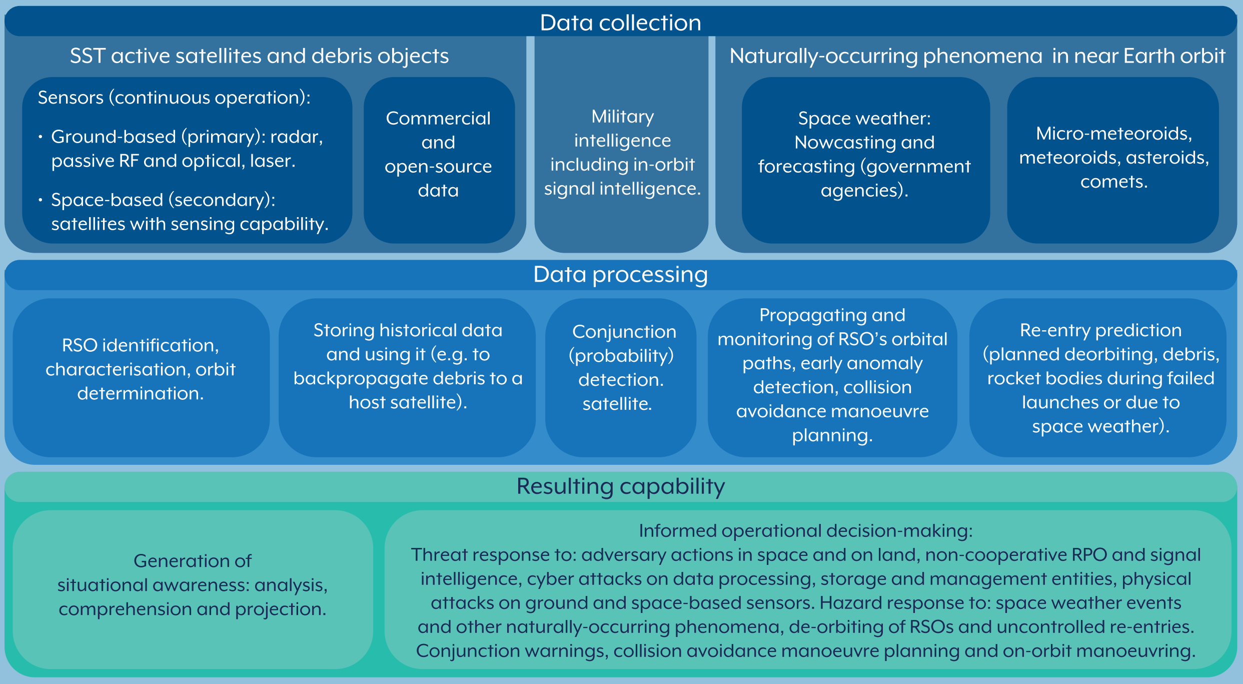
Tasking → Collection → Processing → Analysis → Dissemination

Figures: Space Domain Awareness

The first image below provides additional detail as to the collection and processing of SDA data, specifically:

- The types of data collected
- The ways in which that data is processed and analysed
- The benefits that result from these activities.

The second figure by Kseniia Hryshchuk,3S Northumbria provides an overview of the physical locations and relationships between the elements of SDA components and the external factors that impact on them.



Data collection

SST active satellites and debris objects

Sensors (continuous operation):

- Ground-based (primary): radar, passive RF and optical, laser.
- Space-based (secondary): satellites with sensing capability.

Commercial and open-source data

Military intelligence including in-orbit signal intelligence.

Naturally-occurring phenomena in near Earth orbit

Space weather: Nowcasting and forecasting (government agencies).

Micro-meteoroids, meteoroids, asteroids, comets.

Data processing

RSO identification, characterisation, orbit determination.

Storing historical data and using it (e.g. to backpropagate debris to a host satellite).

Conjunction (probability) detection. satellite.

Propagating and monitoring of RSO's orbital paths, early anomaly detection, collision avoidance manoeuvre planning.

Re-entry prediction (planned deorbiting, debris, rocket bodies during failed launches or due to space weather).

Resulting capability

Generation of situational awareness: analysis, comprehension and projection.

Informed operational decision-making:
Threat response to: adversary actions in space and on land, non-cooperative RPO and signal intelligence, cyber attacks on data processing, storage and management entities, physical attacks on ground and space-based sensors. Hazard response to: space weather events and other naturally-occurring phenomena, de-orbiting of RSOs and uncontrolled re-entries. Conjunction warnings, collision avoidance manoeuvre planning and on-orbit manoeuvring.

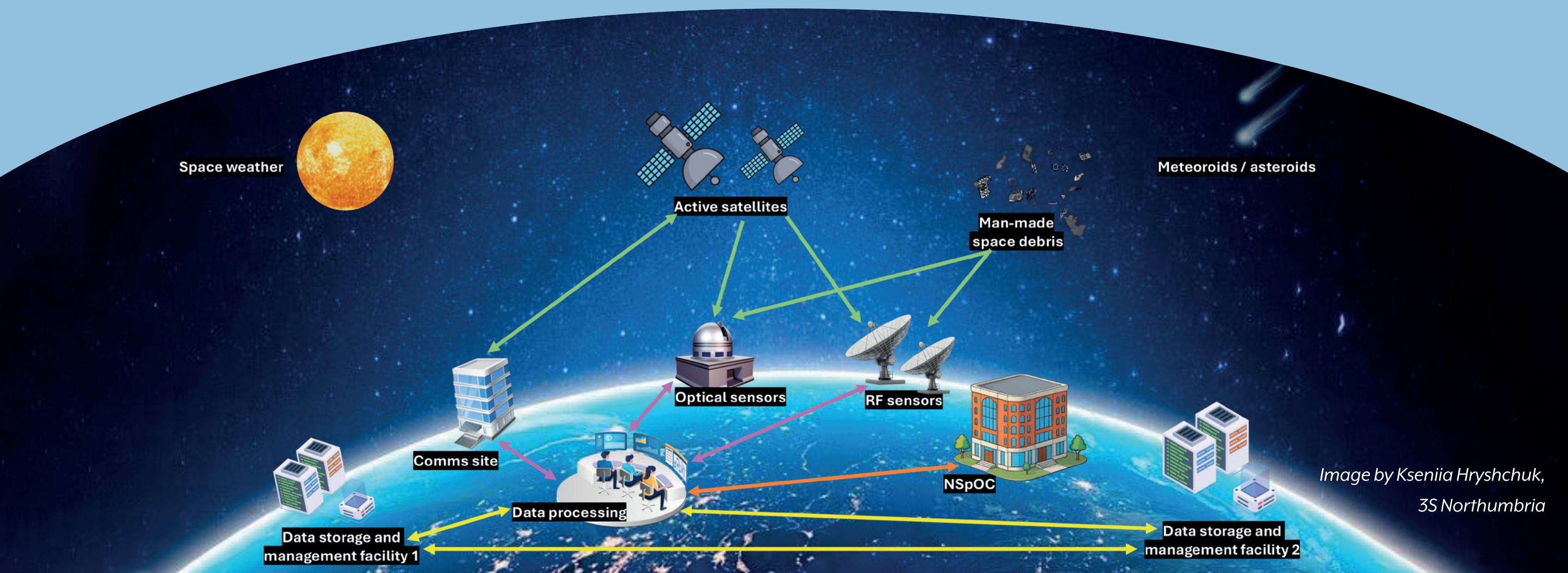


Image by Kseniia Hryshchuk, 3S Northumbria

3. The requirements catalogue

In creating the requirements catalogue, it was decided to start from the structure of the existing Cyber Assessment Framework (CAF), adding in detail to each section that provides context for SDA, and also recognising the aspects of SDA that are not covered in the CAF.

Key points to consider within the catalogue are the disparate activities and actors involved in SDA (including international actors and civil/military cross-over), the specific threats that exist within the space domain, and the impacts on security of the remote nature of space-based assets.

Category	Requirement	Specification	Responsible actors (In UK)	Wider stakeholders
Managing security risk	**Governance**	An understanding of who has overall responsibility for SDA activities, and associated cyber security, and how these interact with international and commercial entities	National Space Operations Centre (NSpOC); UK Space Agency; UK Space Command	UKSpace SDA working group; Key Suppliers; regulators; international organisations, e.g. Combined Space Operations Center (CSpOC)
	Risk management	A full understanding of the risks associated with cyber attacks on SDA assets and systems - likely multiple versions and different classifications	NSpOC; UK Space Agency; UK Space Command	Satellite operators; SDA asset and data providers
	Asset management	A full understanding of every element involved in SDA activities (using project SDA framework as a base), including non-UK based assets, and data transmission and storage across multiple boundaries	NSpOC; UK Space Agency, UK Space Command; SDA sensor, data and analysis providers	Supply chain; international partners
	Supply chain	An understanding of the full supply chain, in terms of both physical assets (sensors, satellites) and data (including processing and analysis. Much of this is international.	NSpOC; UK Space Agency; UK Space Command, SDA sensor, data and analysis providers	International partners
	Data management*	An understanding of the scope and types of data involved in SDA - where it comes from, how it is transmitted and from/to whom, how and by who it is processed, analysed and disseminated - and the ways in which this is managed	NSpOC; UK Space Agency; UK Space Command; commercial SDA providers	Satellite operators; data storage facilities; ground stations
	Communications management*	An understanding of the comms involved in SDA, e.g. tasking, data transmission, shared workplaces for analysis (often international)	NSpOC; UK Space Agency; UK Space Command; commercial SDA providers	Satellite operators; International partners

Category	Requirement	Specification	Responsible actors (In UK)	Wider stakeholders
Protecting against cyber attacks	**Service protection policies, processes and procedures (PPP)**	National (civil and military) PPPs that cover the scope of SDA work in the UK, and are applicable to commercial providers	NSpOC; UK Space Agency; UK Space Command	Commercial SDA providers
	Identity and access Control	A continually managed and updated list of individuals with access to SDA assets (sensors, satellites) and the full data lifecycle. Including military and government personnel, commercial contractors, sensor and satellite manufacturers and operators, and international partners.	NSpOC; UK Space Agency; UK Space Command; Commercial SDA sensor locations; ground stations	Supply chain; international partners
	Data security	Full mapping of the ways in which SDA data can be attacked throughout the lifecycle, and the ways in which it can be protected from these threats.	UK Space Agency; UK Space Command	Commercial SDA providers; international partners; Non-Governmental Organisations (NGOs); Academia
	System security	Full mapping of SDA network and information systems and technology (NSpOC, Space Command, commercial actors), the threats to these systems and the ways they can be attacked. In particular, the challenges associated with the remote nature of space-based assets.	UK Space Agency; UK Space Command	Commercial SDA providers; satellite operators; international partners; NGOs; Academia
	Resilient networks and systems	Processes to build resilience into SDA systems - not just back-ups, but could include multiple connected catalogues, data repositories.	NSpOC; UK Space Agency; UK Space Command	Commercial SDA providers; international partners
	Staff awareness and training	Regular and comprehensive training for all staff, including military and government personnel, contractors and commercial providers, on the importance of cyber security for SDA, impacts and measures that can be taken.	NSpOC; UK Space Agency; UK Space Command	Commercial SDA providers; satellite operators; supply chain
	Remote nature of systems*	An understanding of the additional risks and challenges associated with the remote nature of space-assets and how these will impact the overall cyber security of SDA.	Operators of satellites/ space-based SDA systems	NSpOC; UKSA; UKSC; commercial SDA providers

Category	Requirement	Specification	Responsible actors (In UK)	Wider stakeholders
Detecting cyber security events	**Security monitoring**	Monitoring to detect potential security problems, including loss of data, verification and validation of data.	NSpOC; UK Space Agency; UK Space Command	Commercial SDA providers; international partners
	Proactive security event discovery	An understanding of malicious acts that may fall below the threshold for security monitoring that are specific to SDA and how they might be protected against.	UK Space Agency; UK Space Command	Commercial SDA providers; international partners
	Lack of constant communications*	Analysis of the ways in which the remote nature of ,and lack of constant communication with, many SDA assets can impact security monitoring.	Operators of satellites/ space-based SDA systems	NSpOC; UK Space Agency; UK Space Command
	AI and autonomous defence	Identification of existing or potential that could positively impact cyber security defence.	Industry; academia	NSpOC; UK Space Agency; UK Space Command; commercial SDA providers

Category	Requirement	Specification	Responsible actors (In UK)	Wider stakeholders
Minimising the impact of incidents	**Response and recovery planning**	Mitigation procedures for loss or degradation of all or part of SDA data, or ability to transmit, process or analyse data, e.g. multiple sources of data, analytical tools, sites of analysis, catalogues, and use of partnerships.	NSpOC; UK Space Agency; UK Space Command	Commercial SDA providers; satellite operators; ground stations
	Lessons learned	Processes across all SDA activities and actors to capture and apply learnings from incidents.	NSpOC; UK Space Agency; UK Space Command	Everyone
	Benefits of Space-based Systems*	An analysis of the particulars of space-based systems, such as megaconstellations to provide resilience and the lack of certain attack vectors, that can be used to benefit SDA cyber security processes.	Industry; academia	NSpOC; UK Space Agency; UK Space Command
	AI-based solutions	An understanding of the ways in which AI and autonomy can add resilience into SDA.	Industry; academia	NSpOC; UK Space Agency; UK Space Command

* Asterisks denote additional categories that are outside the existing CAF that it was felt are necessary for SDA

Key points regarding the nature of the catalogue:

- These are high-level cyber-security requirements for SDA, aimed primarily at non-cyber specific individuals, to aid in decision-making and allow for identification of areas where more detail is required
- The catalogue covers general approaches and requirements rather than live threats, focusing on: People, processes and policies; and Governance Structure, which is documented, based on ISO 27k or NIST
- When using the catalogue, it is important to consider the context, both in terms of the realities of space-based infrastructure, and the data being generated, processed, stored and transmitted, and measures that need to be taken into account, such as GDPR and classification
- The catalogue has been developed based on an understanding of the threats to SDA data, and is best used alongside a risk register, mitigations and disaster recovery plans.
- The catalogue assumes that technical standards, such as Cyber Essentials, are adhered to. The recommendation is that lists of standards, such as SPARTA, are made easily available, prime contractors of large projects ensure cyber support to partners such as SMEs, and a 'Secure By Design' approach is promoted.
- It is important to consider how these will be implemented, monitored and maintained in a large system when it becomes operational, and a project team splits up so that consistency is built in.

4. Next steps

Following the initial workshops and the creation of the requirements catalogue, further workshops were held across the UK to map regional capabilities to the catalogue, providing a baseline of what already exists in the UK across the space and cyber sectors to support cyber-security for SDA.

For the next stage in the process, the original working group will come together to use the outputs of the regional workshops and undertake a gap analysis, identifying those areas where either the capability does not exist or there are challenges in implementing capabilities into SDA activities. The final activity within the project will be using these outputs to identify priority areas for investment for the UK and recommendations for a roadmap of activities and procurements.

UK-CYSPACE

FRAZER-NASH
CONSULTANCY
A KBR COMPANY

Frazer-Nash Consultancy Ltd
Hill Park South
Springfield Drive
Leatherhead
Surrey
KT22 7LH

Tel: +44 (0)1306 885050

fnc.co.uk