

Threats to UK space capabilities

Based on the National Risk Register

A report commissioned by the UK Space Agency



Glossary

Acronym	Meaning
ASAT	Anti-Satellite
CCP	Chinese Communist Party
FMECA	Failure Mode, Effects, and Criticality Analysis
ICBM	Intercontinental Ballistic Missile
IR23	Integrated Review Refresh, March 2023
NASA	National Aeronautics and Space Administration
NCSC	National Cyber Security Centre

Contents

Glossary	2
1 Executive Summary	4
Approach	
1.2 Failure Modes and Threats	
1.3 Analysis	
1.4 Comments and next steps	
2 Introduction	7
2.1 Background	
2.2 Scope	
3 Approach	9
3.1 Methodology steps	
3.2 Flow diagram	
3.3 Assessment	
3.4 Data gathering	
4 Space segments and subsystems	15
5 Failure Modes	17
5.1 Physical Destruction	
5.2 Physical Damage	
5.3 Loss of communication	
5.4 Payload Failure	
5.5 Downlink not received	
5.6 Propulsion Failure	
5.7 Deployable Appendage Failure	
5.8 Launch Vehicle Failure	
5.9 Data Processing Error	
6 Threats	27
6.1 Physical threats	
6.2 Electromagnetic threats	
6.3 Cyber threats	
7 Analysis	40
7.1 Threats	
7.2 Failure Modes	
7.3 Space segment analysis	
7.4 Comparisons with the National Risk Register	
8 Closing comments and next steps	47
References	48
Appendix A - Mapping failure modes to threats (tabular)	50
Appendix B - Criticality heat map	53

1 Executive Summary

The 2023 edition of the National Risk Register sets out three risks associated with the space domain, in contrast to just one identified in the 2020 edition of the register. This reflects the situation that modern society is now in, where it is critically reliant on space systems and space-based services for the continued functioning of daily life.

The space domain is abundant with potential threats and hazards, natural and human-made, accidental and intentional. One risk, that of deliberate disruption to UK space systems and space-based services focuses very much on the intentional threats to continued access to and operation within space. This report focuses on this risk, identifying and assessing these threats, cataloguing the failure modes they may cause, and noting the impacts these would have on the operation of space-based systems.

Approach

This report details the application of a modified Failure Mode, Effects, and Criticality Analysis (FMECA) which has been employed to first break down a generic space system into its composite segments, then identify potential failure modes associated with each segment. The FMECA process then allows for the identification of potential threats which may cause each failure mode, and finally an assessment of criticality – the likelihood of a threat occurring and the potential impact if it does. A questionnaire was issued to inform this analysis; responses were received from 9 organisations working across the space domain.



1.2 Failure Modes and Threats

Nine failure modes have been identified, three of which have an impact rating of 5 - Critical, meaning that they may result in a total loss of the spacecraft and/or the mission or operation.

Failure Mode ID	Failure Mode Title	Impact
FM-001	Physical Destruction	5
FM-008	Launch Vehicle Failure	5
FM-004	Payload Failure	5
FM-002	Physical Damage	4
FM-007	Deployable Appendage Failure	4
FM-003	Loss of communications	3
FM-005	Downlink not received	3
FM-006	Propulsion Failure	3
FM-009	Data Processing Error	2

Twelve threats were also identified, one of which has a likelihood rating of 5 – Expected, meaning that the threat is almost certain to occur and may well be encountered already on a near-daily basis.

Threat ID	Threat Category	Threat Title	Likelihood
E-002	Electromagnetic	Downlink jamming	5
E-001	Electromagnetic	Uplink jamming	4
E-003	Electromagnetic	Spoofing	4
C-001	Cyber	Data interception or monitoring	4
C-004	Cyber	Supply chain compromise	4
C-002	Cyber	Data corruption	3
C-003	Cyber	Seizure of control	3
P-002	Physical	Co-orbital	3
P-001	Physical	Direct Ascent ASAT	2
P-003	Physical	Directed Energy	2
P-004	Physical	Ground station incursion or attack	2
P-005	Physical	In-space nuclear detonation	1

1.3 Analysis

This report analyses each threat and failure mode, providing a high-level overview of the potential effects, likely threat actors, and target segments.

It also, by means of a questionnaire distributed to UK space industry stakeholders, provides some commentary of the perception of the risk in industry of deliberate disruption to UK space systems and space-based services. Some key takeaways include:

- Electromagnetic and cyber threats have a higher likelihood of occurrence than physical threats
- It is rare that one failure mode will exist in isolation, and there may be considerable overlap between them
- The link segment is the most vulnerable overall, and most susceptible to electromagnetic and cyber attack
- The level of risk perceived by industry is consistent with the National Risk Register
- Questionnaire respondents representing organisations that own, design, manufacture, operate, or support in-orbit assets perceive a higher impact level than those that do not
- The National Risk Register's reasonable worst-case scenario assumes an attack by a hostile state or proxy, but non-state actors still pose a significant threat

1.4 Comments and next steps

This report presents a high-level analysis into the potential failure modes of UK space systems and services and the possible threat vectors that may result in the realisation of one or more of these failure modes. This report does not investigate or assess any potential mitigation strategies or extant defensive capabilities for preventing the threat.

Furthermore, as a consequence of the high-level nature of this analysis, there may be significant overlap between failure modes and substantial variation in the severity of their potential impacts, depending on the nature and success of the attack, and the capabilities and intent of the threat actor.

It is recommended that future work focuses more closely on decoupling failure modes and attributing them to specific systems and subsystems within each segment. A more detailed FMECA will guide the decision-making process around the assessment and deployment of controls and mitigations to shield UK space systems from the identified threats. Future work should also be undertaken to carry out this process of identifying and developing suitable controls and mitigations. Additionally, any future work employing industry/sector surveys should endeavour to achieve a much larger sample size and the inclusion of respondents from across all of the UK space sector (including military and academia) to present a more accurate summary of stakeholder feedback.

2 Introduction

2.1 Background

The 2020s have seen a rapid increase in geopolitical tensions with significant challenges to the rules-based international order and key flashpoints across the globe.

The UK Government's Integrated Review Refresh published in March 23 (IR23) highlighted that the threat vectors identified in 2021 had become more evident and had accelerated quicker than anticipated, resulting in a period of heightened risk and volatility that is likely to last beyond the 2030s. The IR23 report signalled that China's deepening partnership with Russia and Russia's growing cooperation with Iran in the wake of the invasion of Ukraine are two developments of particular concern. The UK Government's assessment that China under the Chinese Communist Party (CCP) is "an epoch-defining and systemic challenge" and notes its concern that "the CCP's wider goal to achieve regional and global dominance—and the increasingly aggressive means by which it is pursuing this" **(1)**. The National Cyber Security Centre (NCSC) has also warned of a "epoch-defining challenge posed by China", adding that "UK's critical sectors facing 'enduring and significant' threat, in part due to a rise of state-aligned groups and an increase in aggressive cyber activity" **(2)**.

IR23 also recognised that systemic competition is playing out across overlapping strategic arenas, in which there is 'constant and dynamic competition above and below the threshold of armed conflict'. Indeed, the UK 'homebase', its alliances and allies, and the rules-based international order are being persistently challenged by direct and indirect threats that are diversifying, proliferating, and intensifying.



A significant challenge is now coming from the operational space known as the 'Grey Zone'. The UK defines this 'Grey Zone' as coercive activities that "...fall below perceived thresholds for military action and across areas of responsibility of different parts of the government" **(3)**¹. However, as seen in Ukraine, these activities can also take place alongside more conventional military operations where adversaries use an array of capabilities, including their militaries, below (and, occasionally, above) the threshold of armed conflict to operate outside of legal and political norms. Increasingly state adversaries are borrowing techniques from non-state actors and non-state actors are acquiring levels of lethality previously only available to state adversaries. Further, both state and non-state adversaries are adopting similar (overlapping) techniques and disguising their operations across the complex, cluttered, and connected operational domains.

¹ For the rising importance of sub-threshold conflict see David Kilcullen (2020) *The Dragons and the Snakes: How the Rest Learned to Fight the West*, London: Hurst & Co., p. 160-161 and 241.

Modern human society is now critically reliant on near-earth Space based services, the loss of which would lead to rapid economic collapse and civil disorder in days. UK and Allied militaries are likewise dependent on assured access to Space to conduct military operations. The number of objects launched into space continues to rise at unprecedented rates, increasing from 221 objects launched in 2016 to 2664 in 2023 **(4)**, which is reflective of the rapid expansion in the global Space economy.

However, as the current conflict in Ukraine has shown, access to commercially provided Space capabilities can not only provide smaller nations with an asymmetric advantage over great power states but can also be used by non-governmental bodies to attribute acts that contravene international norms. These factors combine to make disruption to military and commercial space systems increasingly attractive to both state and non-state actors. This proliferation in the scale and scope of the threat to Space systems is reflected in the 2023 edition of the National Risk Register which now presents three space-related risks, in contrast to the 2020 edition which considered only the effects of severe space weather.

The space and cyber domains have, and will continue to be, a prime focus for this type of grey zone activity, enabled in part by the massive explosion in connectivity and access to smart platforms and handheld technologies. For example, the technology needed to jam and spoof many types of satellite signals is commercially available and inexpensive, making it relatively easy to proliferate among state and non-state actors, and these attack vectors can produce systemic effects especially if used against a system such as GPS **(5)**.

Additionally, a growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar to those found in non-space systems **(6)**. [For example, on March 1, 2022, unconfirmed reports surfaced that non-state actors affiliated with Anonymous - a decentralized international activist and “hacktivist” collective - hacked their way into Roscosmos’ satellite control centre (5)].

Set against this context, this report focuses on the risk of **deliberate disruption to UK space systems and space-based services** as described in the National Risk Register.

2.2 Scope

This report presents a high-level analysis into the potential failure modes of UK space systems and services and the possible threat vectors that may result in the realisation of one or more of these failure modes. This report does not investigate or assess any potential mitigation strategies or extant defensive capabilities for preventing the threat. Additionally, it does not provide an in-depth assessment of the downstream impacts of a deliberate disruption to UK space capabilities on other sectors and on space-dependent industries. Instead, this analysis focuses primarily on the effects of each failure mode on the space systems themselves and on the services that they provide.

3 Approach



To conduct this analysis, a modified Failure Mode, Effects, and Criticality Analysis (FMECA) has been chosen, to provide a logical framework for the identification of the potential modes of failure for UK space systems and services, and the attribution and assessment of various threats that may induce them.

This methodology also provides a description of the likely impacts of each failure mode and an assessment of their criticality, enabling stakeholders in UK space systems and services to prioritise and target the implementation of safeguards and mitigations.

FMECA is a method often used in the assessment of hardware from the bottom up and on a functional level. However, the complexity of the space domain and interdependent systems within it, coupled with the emphasis on identifying and categorising failure modes, make a modification of FMECA a suitable process for the assessment of threats to UK space systems and services.

3.1 Methodology steps

The modified FMECA methodology contains five key steps:

1. Identification of subsystems and functions

UK space systems are decomposed into their constituent subsystems and grouped by segment (Ground, Space, Link, Launch, and Service). The identification of subsystems and functions allows for clear attribution of failure modes to specific subsystems or more generally, to the segment of space they reside in.

Subsystems and functions can be found in Section 4

2. Identification of failure modes

Taking into account the subsystem breakdown, a list of potential failure modes is identified. This aims to capture ways in which a space system or service may be disrupted. These modes may be temporary or permanent and may be caused by a wide variety of factors.

Failure modes can be found in Section 5

3. Identification of threats

By identifying threats, we aim to capture the mechanisms through which one or more of the failure modes can be realised. Threats to space systems or services can be grouped into three categories, physical, electromagnetic, and cyber. Analysis of the threats indicates their likelihood of occurring and the effect they may have on a space system or service. This threat analysis will also indicate the most likely threat actor(s) to possess the means and motivation to carry out such a threat.

Threats can be found in Section 6

4. Assessment of failure effects

The potential effects of each failure mode are considered, and the likely impact that this would have on the target space system or service itself.

Failure effects can be found in Section 5

5. Determination of criticality

The criticality of each failure mode is assessed, using both the identified failure effects and the likelihood of any threats that are considered to be potential causes of each failure mode. This provides a prioritised list of failure modes, enabling targeted consideration of potential mitigations and countermeasures.

Criticality can be found in Section 7

3.2 Flow diagram

The methodology flow in Figure 3-1 demonstrates the potential many-to-many nature of mapping threats to failure modes.

An argument can be made for linking every identified threat to every identified failure mode. However, this would provide limited utility when trying to discern which threats and which failure modes are of most interest. Where possible, the linkages between threats and failure modes have been made where a reasonable case can be put forward that a particular threat could be deployed primarily to bring about a particular failure mode.

By way of an example, threat P-001 Direct Ascent ASAT could be deployed to trigger failure mode FM-001 Physical Destruction. This in turn would automatically result in the realisation of FM-003 Loss of communication and FM-005 Downlink not received. However, as the primary goal of any threat actor launching a direct ascent ASAT would likely be the destruction of its target, rather than simply disabling its communications, no linkage would be drawn between P-001 and FM-003 & FM-005.

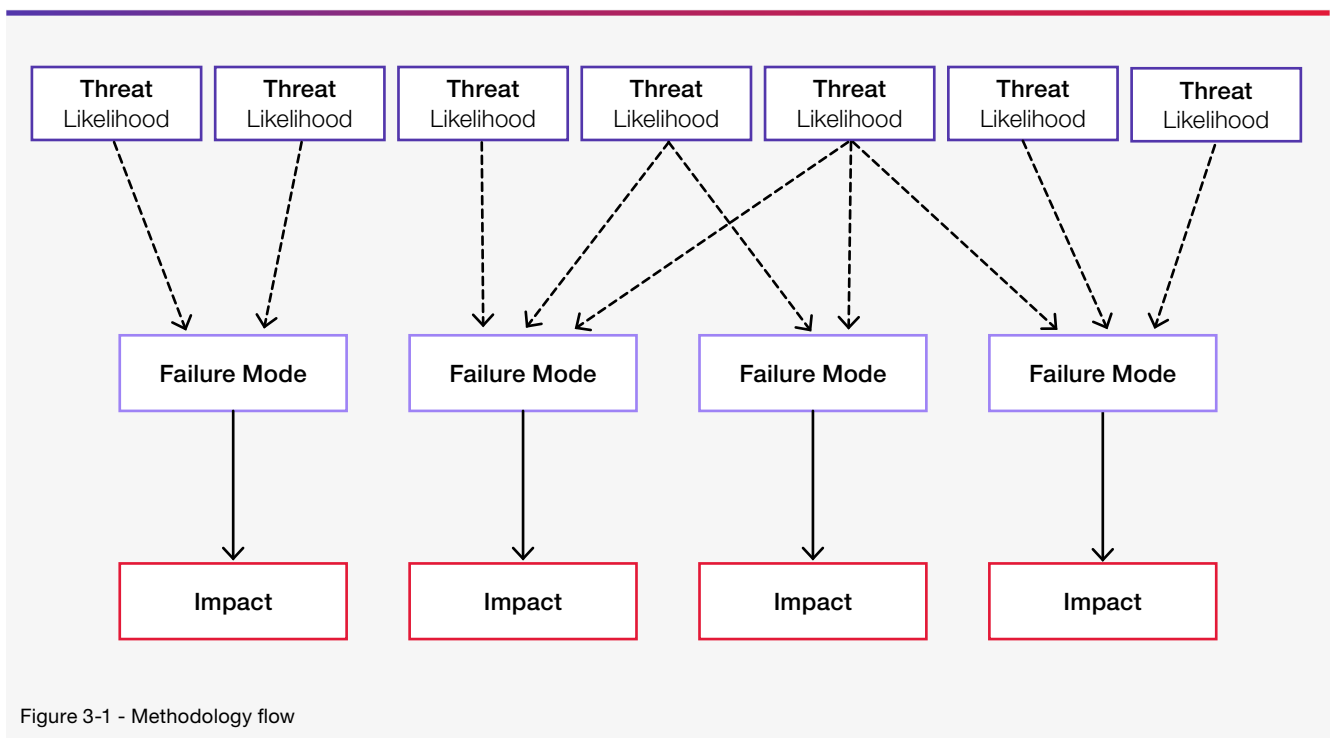


Figure 3-1 - Methodology flow

3.3 Assessment

3.3.1 Criticality

Assessment of criticality is adapted from NASA's Standard for Performing a Failure Modes and Effects Analysis (7), using a qualitative assessment of threat likelihood and an amalgamation of hardware impact and mission impact from the NASA document to derive failure mode impact.

Assessment of the likelihood of a threat occurring, and the impact of a failure mode is displayed on a scale of 1-5, using the criteria listed below:

	Threat Likelihood	Failure Mode Impact
1	Slight – There is a remote chance of the event occurring	No Impact – No damage to spacecraft or impact to the mission or operation capability
2	Not Likely – The event is possible but unlikely to occur	Minor Impact – Limited disruption to operation
3	Likely – It is likely that the event will occur	Moderate Impact – Significant damage to spacecraft or loss of mission or operation capabilities
4	Highly Likely – It is highly likely that the event will occur	Serious Impact – Major damage to spacecraft or loss of mission or operation capabilities
5	Expected – The event is almost certain to occur	Critical Impact – Total loss of the mission or operation

3.3.2 Threat actors

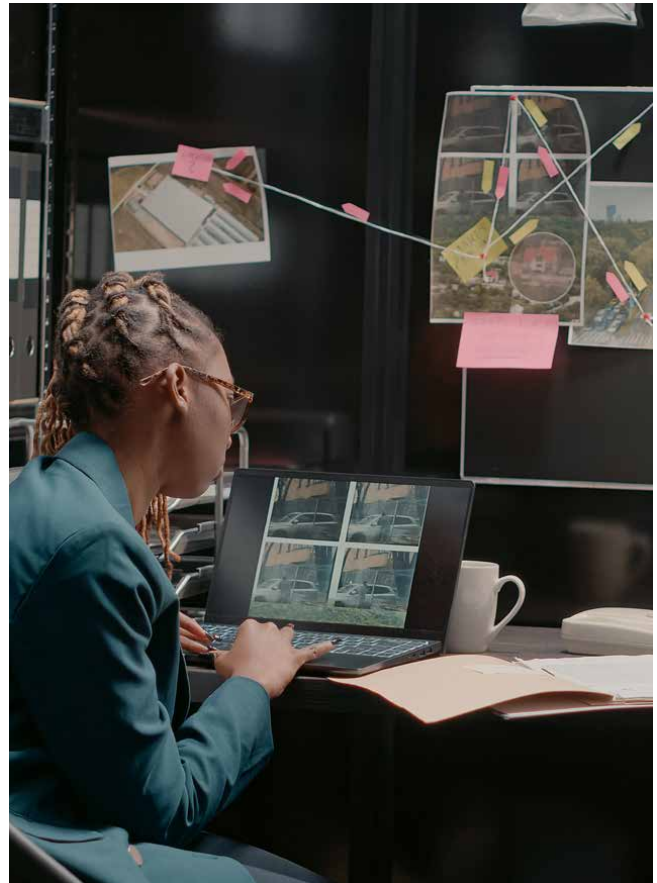
Threat actors are the individuals, groups, organisations, or nation-states who pose the threat.

When assessing possible threat actors, consideration should be given to the likely objectives of the threat. The threat actors' objectives may range from simple probing to determine what instant impact they can have on a system, to gathering intelligence for antagonistic use at a future time.

Additionally, understanding the resources required to carry out the threat will help to determine likely threat actors. The resources that threat actors have to perform an attack may range between being limited, such as in the case of thrill seekers, to very extensive, in the case of antagonistic nation-states and organised cybercriminals.

The following threat actors were considered for this assessment:

- **Cyber criminals** – primarily motivated by financial gain
- **Idealogues (hacktivists, terrorists)** – motivated by ideology may use attacks to spread their message (hacktivists) or to cause terror and destruction (terrorists)
- **Insiders/Competitors** – disgruntled employees leaking information for revenge or monetary gain and competitors seeking to gain competitive advantage
- **Nation-states** – aim to gather intelligence or cause disruption or destruction of critical national infrastructure
- **Thrill seekers/Trolls** – testing their abilities to infiltrate a system or cause disruption



3.4 Data gathering

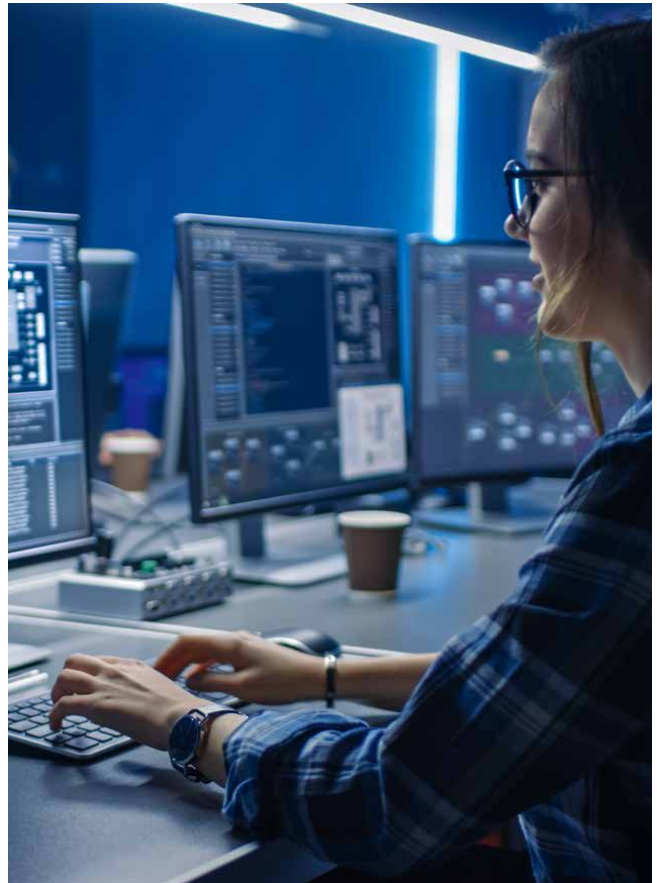
To supplement the information gained through extensive literature review and CGI's in-house expertise in the space and cyber security domains, a questionnaire has been issued to the broader UK space industry. This questionnaire aimed to capture the opinions and insights of those working in the design, manufacturing, operation, or support of space-based systems as well as industry experts.

Qualitative data from this questionnaire has informed the general tone and content of the document.

Quantitative data from the questionnaire has been used to generate the Most likely threat category charts in Section 5 as well as the space segment analysis in Section 7.3 and comparison against the National Risk Register in Section 7.4

At time of publishing, responses to the questionnaire have been received from the following organisations:

- SJE Space Ltd
- Raytheon UK
- MDA UK
- Serco
- Inverse Quanta Ltd
- Methera Global Communications Ltd
- Telespazio UK Ltd
- e2E Services
- CGI IT UK Ltd

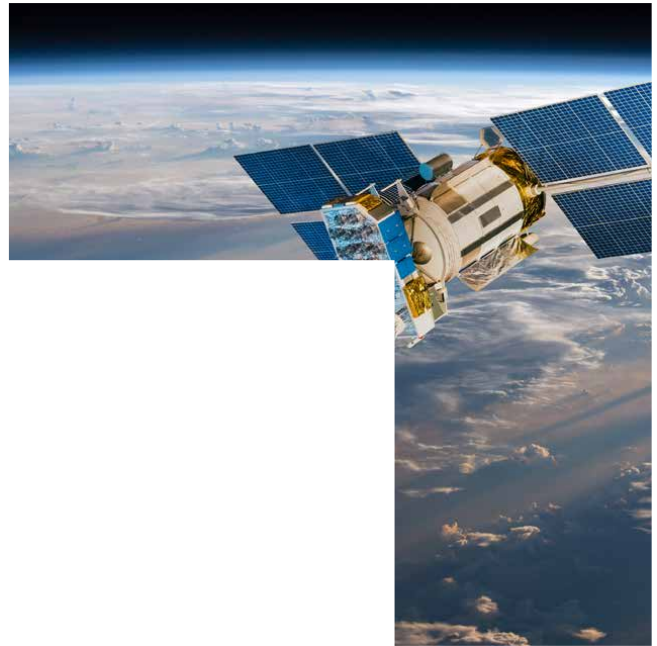


4 Space segments and subsystems

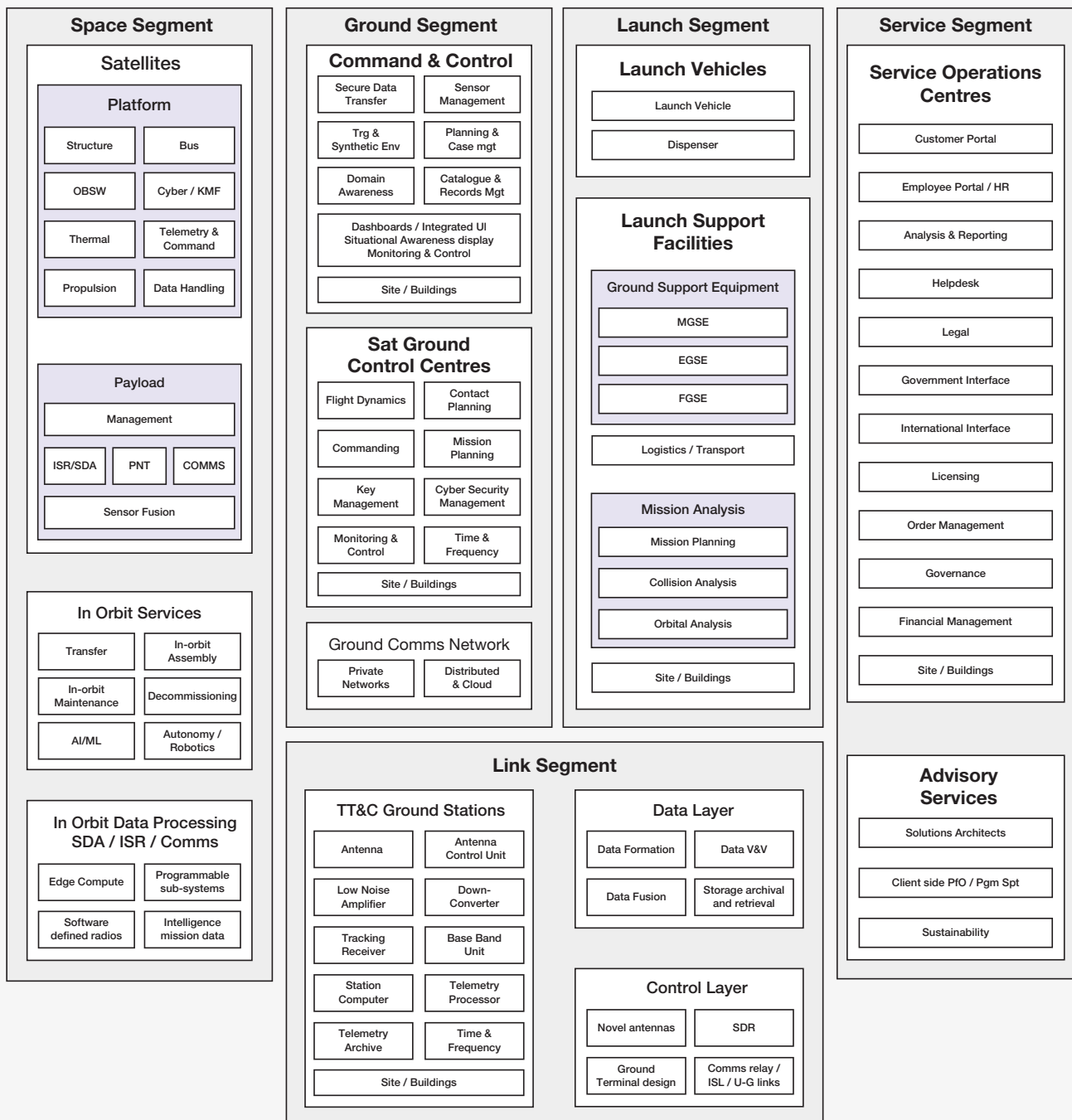
For the purpose of this analysis, a generic space system has been broken down into five segments, building on the Space Technology framework set out by In-Q-Tel (8). Each segment contains a summary of the various subsystems that make up a generic space system, and the functions that these subsystems perform.

This breakdown is used to attribute potential failure modes and likely threat vectors to each segment, identifying which segments are most susceptible to different types of attack and allowing for the consideration and implementation of sufficient threat mitigation and avoidance measures. These measures are not discussed within this report. The breakdown describes the following segments:

- **Space segment** - Containing all in-orbit assets, comprising the satellite platform and its payload as well as in-orbit services such as in-orbit manufacturing, maintenance, orbit transfer, and decommissioning
- **Ground segment** - All ground infrastructure related to the command and control of the satellite mission, mission planning, ground station communication and data storage
- **Link segment** - Including all signals sent between in-orbit and ground assets, and all equipment required to transmit and process this data
- **Launch segment** - Comprising the launch vehicle and launch support facilities
- **Service segment** - Including interfaces between the mission and end users/governments, all licensing and compliance activities and other service operations



Space System by Segment



5 Failure modes



Nine failure modes have so far been identified which aim to capture ways in which a space mission may fail. These modes may be temporary or permanent and may be caused by a wide variety of factors. This analysis considers only the deliberate causes of these failure modes. These causes are termed threats and are detailed in Section 6.

The nine identified Failure Modes are:

FM-001 Physical Destruction

FM-002 Physical Damage

FM-003 Loss of communication

FM-004 Payload Failure

FM-005 Downlink not received


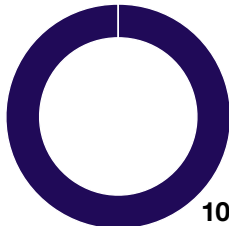
FM-006 Propulsion Failure

FM-007 Deployable Appendage Failure


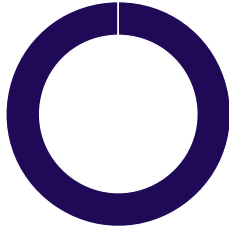
FM-008 Launch Vehicle Failure

FM-009 Data Processing Error


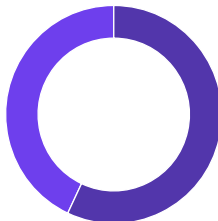
5.1 Physical Destruction

	FM-001	Physical Destruction	Impact				
			1	2	3	4	5
The satellite and payload are physically destroyed, resulting in a total loss.							
Summary of Effects			Possible Threats				
<p>By far the most dramatic and irreversible of the identified failure modes, a reasonable worst-case scenario of physical destruction of a satellite and its payload would result in the total loss of the asset and immediate cessation of its contribution to its mission or operation.</p> <p>Assuming a scenario where the satellite structure is destroyed rather than disabled, the destruction event may cause additional damage to other assets in proximity from the resulting debris field. This could also provide the trigger for a possible Kessler collisional cascade. This effect may be mitigated by the spatial separation of the affected satellite and others.</p> <p>The mission or operation to which the destroyed satellite belonged may be significantly disrupted, degraded, or in some cases brought to a premature and permanent end. This effect may be mitigated if the destroyed satellite is part of a constellation that can accommodate the loss of one of its members. Nevertheless, there may be a delay in service or availability whilst a replacement satellite is launched or whilst the constellation adapts to the loss.</p>			<p>P-001 Direct Ascent ASAT</p> <p>P-002 Co-orbital</p> <p>P-003 Directed Energy</p> <p>P-004 Ground station incursion</p> <p>P-005 In-space nuclear detonation</p> <p>C-003 Seizure of control</p>				
			Most likely threat category				
			 <p>100%</p> <div><div></div>Physical</div> <div><div></div>Electromagnetic</div> <div><div></div>Cyber</div>				

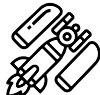
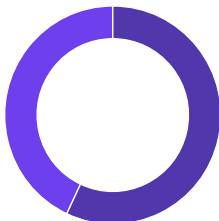
5.2 Physical Damage

	FM-002	Physical Damage	Impact						
			1	2	3	4	5		
The satellite bus or payload is physically damaged									
Summary of Effects				Possible Threats					
<p>A similar but less severe failure mode to the previous FM-001, a reasonable worst-case scenario would result in the damage to some components of the satellite or payload, stopping short of a total loss. A wide range of effects can be expected as result of this failure mode, depending heavily on the location and extent of damage, and the satellite’s ability to continue to operate, albeit in a degraded manner.</p> <p>For modular systems, an in-orbit repair or replacement of parts may be possible, subject to the development and availability of in-orbit servicing capabilities. Likewise for satellites that operate as part of a constellation, the effect on the mission or operation may be mitigated by burden sharing across the remainder of the constellation.</p> <p>There may be significant overlap between this failure mode and the following: FM-003 Loss of communication, FM-004 Payload Failure, FM-006 Propulsion Failure, and FM-007 Deployable Appendage Failure.</p>				<p>P-001 Direct Ascent ASAT</p> <p>P-002 Co-orbital</p> <p>P-003 Directed Energy</p> <p>P-004 Ground station incursion</p> <p>P-005 In-space nuclear detonation</p> <p>C-003 Seizure of control</p> <p>C-004 Supply chain compromise</p>					
				Most likely threat category					
				 <div>100%</div>					
				<div><div></div>Physical</div> <div><div></div>Electromagnetic</div> <div><div></div>Cyber</div>					


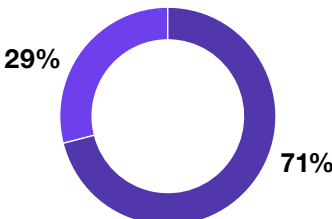
5.3 Loss of communication

	FM-003	Loss of communication	Impact				
			1	2	3	4	5
Communication is lost with the satellite, rendering it unresponsive							
Summary of Effects				Possible Threats			
<p>The primary effects of a loss of communication with a satellite are the inability to issue commands, manoeuvre, and monitor system status. The inability to command the propulsion system and thus manoeuvre the satellite may render it unable to effectively station-keep, move to its operational area or orbit, and crucially carry out avoidance manoeuvres in response to hazards or potential conjunction events. This may be mitigated if the satellite is able to operate autonomously with a reduced reliance on commands issued from the ground.</p> <p>A temporary loss of communication may result in the satellite not being in its required operational area at specific times, interrupting or degrading the service it provides, or may see it move beyond its intended orbit parameters, requiring additional fuel spend to reposition once communication is re-established.</p> <p>A permanent loss of communication may result in the satellite becoming a hazard to other spacecraft, as its status can no longer be monitored and its ability to manoeuvre removed.</p> <p>Depending on the nature of the issue and its cause, a loss of communication may also result in downlink signals not being received (FM-005).</p>				<p>P-002 Co-orbital</p> <p>P-003 Directed Energy</p> <p>P-004 Ground station incursion</p> <p>E-001 Uplink jamming</p> <p>E-002 Downlink jamming</p> <p>E-003 Spoofing</p> <p>C-001 Data interception</p> <p>C-002 Data corruption</p> <p>C-003 Seizure of control</p> <p>C-004 Supply chain compromise</p>			
				Most likely threat category			
				<div><div><div>43%</div><div></div><div>57%</div></div><div><div></div>Physical</div><div><div></div>Electromagnetic</div><div><div></div>Cyber</div></div>			


5.4 Payload Failure

	FM-004	Payload Failure	Impact				
			1	2	3	4	5
The mission payload suffers a deployment or operational failure, resulting in an inability to gather or transmit mission data							
Summary of Effects			Possible Threats				
<p>The effects of a payload failure will be largely confined to the success of the mission or operation, rather than presenting a physical hazard to itself and other spacecraft. A failure of the payload to deploy or otherwise function as intended may result in operational or mission data not being collected, being only partially collected and of limited utility, or not being transmitted back to Earth.</p> <p>Depending on the mission or operation, this may have additional impacts downstream, ranging from the disruption or cessation of scientific experiments to severe disruption to terrestrial systems in the case of a positioning or timing failure, or non-receipt of communications signals.</p> <p>The effects of a payload failure may be partially or fully mitigated depending on the nature of the mission and failure by any redundancy built in either onboard the affected satellite or as part of a larger constellation, or if deemed significant enough, through in-orbit maintenance and repair.</p>			<p>P-002 Co-orbital</p> <p>P-003 Directed Energy</p> <p>E-001 Uplink jamming</p> <p>E-003 Spoofing</p> <p>C-003 Seizure of control</p> <p>C-004 Supply chain compromise</p>				
			Most likely threat category				
			<div><div>43%</div><div></div><div>57%</div></div> <div><div><div></div>Physical</div><div><div></div>Electromagnetic</div><div><div></div>Cyber</div></div>				


5.5 Downlink not received

	FM-005	Downlink not received	Impact										
			1	2	3	4	5						
Mission or operational data is not received by the ground station													
Summary of Effects				Possible Threats									
<p>Non-receipt of a downlink signal may cause disruption to an operation or a mission by preventing the processing and distribution of essential data, affecting its integrity or reliability. Whilst unlikely to result in damage to the spacecraft, or create additional hazards in orbit, without the ability to receive the downlink, it is unlikely that the purpose of the satellite, regardless of its mission or operational type, can be fulfilled.</p> <p>The effects are unlikely to be permanent and will persist for as long as the source of the failure is active, however during this time the mission or operation may be wholly or partially compromised. Depending on the nature of the mission or operation, effects to end-users may include the disruption of satellite communication, issues with positioning and navigation services, gaps in data collected for scientific observations, or an inability to access satellite-enabled broadband.</p> <p>Depending on the nature of the threat, this failure mode may affect a single satellite or the downlink from multiple satellites directed at the same ground station. Whilst the impact may be high for the duration of the failure, its reversibility and general lack of collateral damage means that non-receipt of a downlink signal is unlikely to cause a significant or critical loss of capability.</p>				<p>P-002 Co-orbital</p> <p>P-003 Directed Energy</p> <p>P-004 Ground station incursion/ attack</p> <p>P-005 In-space nuclear detonation</p> <p>E-002 Downlink jamming</p> <p>E-003 Spoofing</p> <p>C-001 Data interception</p> <p>C-002 Data corruption</p> <p>C-003 Seizure of control</p> <p>C-004 Supply chain compromise</p>									
				Most likely threat category									
				 <table><tr><td>Physical</td><td>29%</td></tr><tr><td>Electromagnetic</td><td>71%</td></tr><tr><td>Cyber</td><td>0%</td></tr></table>				Physical	29%	Electromagnetic	71%	Cyber	0%
Physical	29%												
Electromagnetic	71%												
Cyber	0%												


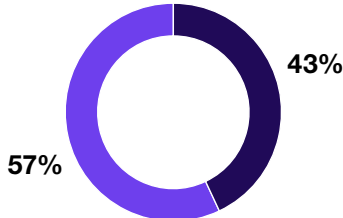
5.6 Propulsion Failure

	FM-006	Propulsion Failure	Impact												
			1	2	3	4	5								
The on-board propulsion system fails, resulting in a degradation or loss of manoeuvrability															
<h3>Summary of Effects</h3> <p>A failure of the propulsion system would result in a full or partial loss of manoeuvrability, and if permanent would likely result in a premature cessation of the mission or operation, as the spacecraft would be unable to change or maintain its position.</p> <p>In this scenario, the unresponsive spacecraft would eventually deorbit, albeit with no means to control or manage its descent or may become a hazard to other spacecraft as an object involved in a potential conjunction event.</p> <p>A temporary failure to the propulsion system would result in largely reversible effects, and upon restoration of the propulsion system, the spacecraft would once again be able to manoeuvre in order to station-keep or reach its operational area. However, the craft may have diverged from its expected orbit or position in the time taken to restore the propulsion system and as a result, increased fuel burn may be required to set it back on course.</p> <p>There is considerable potential overlap with FM-007, as the failure to deploy an appendage such as a solar array may deprive the spacecraft of power, thus resulting in a failure of the propulsion system.</p>				<h3>Possible Threats</h3> <p>P-002 Co-orbital</p> <p>P-003 Directed Energy</p> <p>E-001 Uplink jamming</p> <p>E-003 Spoofing</p> <p>C-003 Seizure of control</p> <p>C-004 Supply chain compromise</p>											
				<h3>Most likely threat category</h3> <table><thead><tr><th>Category</th><th>Percentage</th></tr></thead><tbody><tr><td>Physical</td><td>14%</td></tr><tr><td>Electromagnetic</td><td>71%</td></tr><tr><td>Cyber</td><td>14%</td></tr></tbody></table> <ul style="list-style-type: none">PhysicalElectromagneticCyber				Category	Percentage	Physical	14%	Electromagnetic	71%	Cyber	14%
Category	Percentage														
Physical	14%														
Electromagnetic	71%														
Cyber	14%														



5.7 Deployable Appendage Failure

	FM-007	Deployable Appendage Failure	Impact										
			1	2	3	4	5						
Components such as solar arrays, antennae, or transmitters fail to deploy													
Summary of Effects				Possible Threats									
<p>Deployable appendages are critical components of spacecraft, and a successful space mission or operation often hinges on their ability to function. Depending on the intended function of the spacecraft, it may carry deployable appendages such as solar arrays, antennas, telescopes, transmitters, or other sensing equipment. Failure of these components therefore, depending on the nature of the appendage and the severity of the failure, could result in an inability to complete the mission or operational objectives and may bring the mission or operation to a premature end.</p> <p>Failure to complete objectives can often prompt large insurance claims, with NASA estimating a total of almost \$800m in insurance claims resulting from failed deployments of solar arrays alone in the period 1994-2017 (9).</p> <p>There is potential overlap with FM-004, FM-005, and FM-006, as this may result in a failure to deploy the payload, an inability to transmit data back to Earth due to a fault with on-board antennae, or a failure of the propulsion system as a result of undeployed solar arrays.</p> <p>In rare cases, a deployable appendage failure may be resolved upon release from the launch vehicle, although with the majority of launches now uncrewed, this is unlikely to be the case. Previous examples of manual intervention to initiate deployment are largely confined to spacecraft launched from the Space Shuttle. In 1984, crew of STS-41G were able to free a stuck solar panel of the Earth Radiation Budget Satellite and in 1991 crew onboard STS-37 undertook an Extra-Vehicular Activity (EVA) to deploy the Gamma Ray Observatory.</p> <p>In the future, this type of failure may be partially or wholly mitigated with the use of robotic in-orbit servicing spacecraft, however in the interim it remains a failure mode with the potential to critically disrupt or degrade a spacecraft mission or operation.</p>				<p>P-002 Co-orbital</p> <p>P-003 Directed Energy</p> <p>E-001 Uplink jamming</p> <p>E-003 Spoofing</p> <p>C-003 Seizure of control</p> <p>C-004 Supply chain compromise</p>									
				Most likely threat category									
				A donut chart showing the distribution of threat categories. The chart is divided into two segments: a larger purple segment representing 71% and a smaller dark blue segment representing 29%. <table><tr><th>Threat Category</th><th>Percentage</th></tr><tr><td>Physical</td><td>29%</td></tr><tr><td>Electromagnetic</td><td>71%</td></tr></table>				Threat Category	Percentage	Physical	29%	Electromagnetic	71%
Threat Category	Percentage												
Physical	29%												
Electromagnetic	71%												
				<ul style="list-style-type: none">PhysicalElectromagneticCyber									

5.8 Launch Vehicle Failure

	FM-008	Launch Vehicle Failure	Impact				
			1	2	3	4	5
Malfunction or loss of launch vehicle							
<h3>Summary of Effects</h3>				<h3>Possible Threats</h3>			
<p>A failure of the launch vehicle will almost always result in the total loss of itself and its payload. Less commonly, a launch vehicle may successfully reach its intended deployment area but suffer an issue with the deploying its payload.</p> <p>Whilst there are no recorded examples of a launch vehicle failing due to a deliberate attack, numerous examples of unintentional launch vehicle failure or loss do exist, including the recent loss of Virgin Orbit’s LauncherOne which was destroyed along with its payload of nine satellites shortly after launch from Spaceport Cornwall in January 2023 (10).</p> <p>In addition to the loss of the launcher and its payload, this failure mode may result in a delay to future launches, whilst an investigation into the cause of the failure is carried out and whilst a replacement launcher and payload are manufactured or sourced. This failure mode is unlikely to result in a loss or decrease in mission or operational capability as the launched asset will not have yet entered service, however depending on the nature of the intended payload this may result in a delay in upgrading an existing space-based service or in commissioning a new one.</p>				<p>P-005 In-space nuclear detonation</p> <p>C-003 Seizure of control</p>			
				<h3>Most likely threat category</h3>			
							
				<div><div></div> Physical</div> <div><div></div> Electromagnetic</div> <div><div></div> Cyber</div>			

5.9 Data Processing Error

	FM-009	Data Processing Error	Impact				
			1	2	3	4	5
Data processed in the ground segment is corrupted, incorrect, or otherwise unusable resulting in false conclusions or lack of usability of data							
Summary of Effects			Possible Threats				
<p>An error in the processing of data received from the spacecraft or from other ground stations could have a litany of causes, both deliberate and non-deliberate. In most cases the error and its cause will be quickly identified and rectified, resulting in perhaps significant but limited disruption to the operation or mission.</p> <p>Incorrect data may lead to false conclusions being derived about the status or position of the spacecraft, or by end-users of the data which may range from scientific experiments to the routine operation of broadcasting and communications networks, or positioning and navigation services.</p> <p>The effects of this failure mode can be mitigated with robust error checking once data is received and processed by the ground station. This may identify anomalies in the data and prevent the release of incorrect data to its end-users. However, this will result in the data being unusable which may still trigger outages in systems reliant on the data or delays in operations or experiments utilising it.</p>			<p>P-004 Ground station incursion/ attack</p> <p>E-001 Uplink jamming</p> <p>E-002 Downlink jamming</p> <p>E-003 Spoofing</p> <p>C-001 Data interception</p> <p>C-002 Data corruption</p> <p>C-004 Supply chain compromise</p>				
			Most likely threat category				
			<div><p>100%</p><div><div></div>Physical<div></div>Electromagnetic<div></div>Cyber</div></div>				

6 Threats



Twelve threats have been identified during the course of this analysis, and have been grouped into three categories: physical, electromagnetic, and cyber.

Physical threats

- **P-001** Direct Ascent ASAT
- **P-002** Co-orbital
- **P-003** Directed Energy
- **P-004** Ground station attack or incursion
- **P-005** In-space nuclear detonation

Electromagnetic threats


- **E-001** Uplink jamming
- **E-002** Downlink jamming
- **E-003** Spoofing

Cyber threats


- **C-001** Data Interception or Monitoring
- **C-002** Data Corruption
- **C-003** Seizure of Control
- **C-004** Supply Chain Compromise

6.1 Physical threats


6.1.1 Direct Ascent ASAT

	P-001	Direct Ascent ASAT	Likelihood				
			1	2	3	4	5
Weapons that use ground, air-, or sea-launched missiles with interceptors that are used to kinetically destroy satellites through force of impact, but are not placed into orbit themselves							
Analysis			Threat Actors				
<p>The use of ground, air, or sea launched missiles to intercept and destroy satellites is well-established, although no overtly hostile activities have taken place to date. China, India, Russia, and the United States have all carried out ASAT tests on their own satellites.</p> <p>The primary effects are the total destruction of or damage to the target satellite. This impact, however, creates a large debris field and therefore a secondary threat to many other space assets in proximity to the target satellite. For instance, the 2021 Russian destruction of Cosmos-1408 generated nearly 1800 pieces of trackable debris, and undoubtedly many smaller and non-trackable pieces that still pose a significant threat to other satellites and space assets.</p> <p>The creation of large numbers of uncontrollable pieces of space debris and the hazards to spacecraft that they pose has led to an international effort to halt the testing of direct ascent ASAT's. In 2022 the United Nations General Assembly approved a resolution put forward by the United States to do this. However, this is likely to be a largely symbolic measure, with the resolution being opposed or abstained from by the other three nations that have to date, carried out such tests, and additionally by Belarus, Bolivia, Cuba, Iran, Nicaragua, Syria, and the Central African Republic.</p> <p>Whilst there is historical precedent confirming the capability of nation-states to deploy direct ascent ASATs against the space assets of other nations, this kind of direct hostile action would likely cross the threshold for a military response and could result in significant consequences for the aggressor. Given the availability of other, sub-threshold activities, to disrupt or degrade space capabilities, this threat is therefore considered unlikely except as part of a larger scale international state-on-state armed conflict.</p>			• Nation-states				
			Related Failure Modes				
			• FM-001 Physical Destruction				
			• FM-002 Physical Damage				
			Most susceptible segments				
• Space							
Selected Incidents							
<p>This list details successful ASAT tests, resulting in direct contact with a target satellite and the creation of a debris field (11):</p> <ul style="list-style-type: none">• 1985 USA (Sol wind)• 2007 China (FengYun 1C)• 2008 USA (USA-193)• 2019 India (Microsat-R)• 2021 Russia (Cosmos-1408)							


6.1.2 Co-orbital

	P-002	Co-orbital	Likelihood				
			1	2	3	4	5
Weapons that are placed into orbit and then manoeuvre to approach the target to attack it by various means, including destructive and non-destructive							
Analysis			Threat Actors				
<p>Co-orbital systems, in contrast to Direct Ascent ASAT's, offer the potential to engage in prolonged sub-threshold activity with both destructive and non-destructive capabilities.</p> <p>The development of co-orbital anti-satellite capabilities is not new, and their origins can be traced back to the Soviet Istrebitel Sputnikov (IS) programme of the 1970s and 1980s (12). This system followed largely the same principle as the United States' cancelled Multiple Kill Vehicle of the mid-2000s in that a warhead would be deployed into orbit and then manoeuvre to attack its target. In the case of the IS system, the target would be another satellite and for the Multiple Kill Vehicle it would be hostile Intercontinental Ballistic Missiles (ICBM's).</p> <p>However, the non-destructive potential of co-orbital capabilities is likely to be the focus of possible future deployment. In this scenario, hostile co-orbital satellites may shadow their target, seeking to either disrupt or intercept communications to and from whilst remaining as inconspicuous as possible. In 2020 the United States alleged that the Russian Cosmos-2519, an inspection satellite, behaved "inconsistently" with its intended mission (13). This followed an incident in 2019 when Russian satellites Cosmos-2542 and Cosmos-2543 were accused by the commander of US Space Force of manoeuvring close to and within 100 miles of the US reconnaissance satellite KH-11 (14).</p> <p>This ability to carry out sub-threshold activities against satellites and other space assets therefore makes the likelihood of a co-orbital attack, either destructive or non-destructive, likely in the short to medium term.</p>			<ul style="list-style-type: none">• Nation-states				
			Related Failure Modes				
			<ul style="list-style-type: none">• FM-001 Physical Destruction• FM-002 Physical Damage• FM-003 Loss of communication• FM-004 Payload Failure• FM-005 Downlink not received• FM-006 Propulsion Failure• FM-007 Deployable Appendage Failure				
			Most susceptible segments				
			<ul style="list-style-type: none">• Space				
			Selected Incidents				
			<ul style="list-style-type: none">• 2019 Russian Cosmos-2542 and Cosmos-2543 (14)• 2020 Russian Cosmos-2519 (13)				


6.1.3 Directed Energy

	P-003	Directed Energy	Likelihood				
			1	2	3	4	5
Weapons that use focused energy, such as laser, particle, or microwave beams to interfere with or destroy space systems							
Analysis			Threat Actors				
<p>Directed Energy covers a range of weapons that use highly focused energy to damage their target rather than the use of a solid projectile. The focused energy can take multiple forms, including lasers, high frequency microwaves, particle beams, and sound energy. In contrast to Direct Ascent ASAT's, directed energy weapons have the potential to be used more discreetly, generating no sound (unless desired) and no visible trace, except potentially heat signatures.</p> <p>The damage caused by directed energy weapons can vary, depending on the intent and capability of the attacker. Laser systems can temporarily or permanently blind on-board sensing equipment whilst high frequency microwaves may damage or destroy on-board electrical systems. Whilst not requiring the same level of logistical organisation as a direct ascent ASAT, with no requirement for launching capabilities or the supply of ammunition, directed energy weapons nonetheless are advanced systems to manufacture, operate, and target, putting them likely beyond the reach of most non-state actor adversaries.</p> <p>To date, there have been no recorded incidents of directed energy weapons being used in a hostile manner, and the technology is currently in its infancy. However, the deployment by Russia in 2019 of Peresvet laser systems, which it claims are designed to blind enemy ground and space based optical tracking systems, to five of its strategic missile divisions, as well as allegations by the United States that China already possesses multiple ground-based laser weapons with anti-satellite capabilities (15), suggests the likelihood of this kind of weaponry seeing active use in the future is high.</p>			• Nation-states				
			Related Failure Modes				
			• FM-001 Physical Destruction				
			• FM-002 Physical Damage				
			• FM-003 Loss of communication				
• FM-004 Payload Failure							
• FM-005 Downlink not received							
• FM-006 Propulsion Failure							
• FM-007 Deployable Appendage Failure							
			Most susceptible segments				
			• Space				
			Selected Incidents				
			None				

6.1.4 Ground station attack or incursion

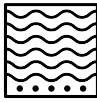
	P-004	Ground station attack or incursion	Likelihood				
			1	2	3	4	5
<p>Physical attack or breach of ground station which may present danger to life of staff and result in seizure of control or unauthorised access to telemetry data. It can also be the enabling event for a disruptive cyber operation.</p>							
<h3>Analysis</h3>			<h3>Threat Actors</h3> <ul style="list-style-type: none">• Idealogues• Cybercriminals• Insiders/Competitors <h3>Related Failure Modes</h3> <ul style="list-style-type: none">• FM-001 Physical Destruction• FM-002 Physical Damage• FM-003 Loss of communication• FM-005 Downlink not received• FM-009 Data Processing Error• FM-007 Deployable Appendage Failure <h3>Most susceptible segments</h3> <ul style="list-style-type: none">• Ground <h3>Selected Incidents</h3> <ul style="list-style-type: none">• 1992 Rockwell International GPS attack (16)				

6.1.5 In-space nuclear detonation

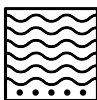
	P-005	In-space nuclear detonation	Likelihood				
			1	2	3	4	5
<p>A nuclear detonation in space, which may have a wide area of effect and no specific target. May cause an electromagnetic pulse, transient nuclear radiation, disruption to the ionosphere affecting communications, or thermal radiation damage to many assets.</p>							
Analysis			Threat Actors				
<p>In the vacuum of space, it is not the kinetic impact of a nuclear detonation that poses the biggest threat, but the rapid and intense release of radiation that may cause an electromagnetic pulse, create a temporary radiation belt, or damage components onboard spacecraft due to intense heat exposure. The possible effects of such an event would vary wildly, depending on the proximity of the detonation to space assets, the orbit in which the detonation occurs, and the yield of the blast.</p> <p>Whilst the likelihood of a deliberate nuclear detonation being carried out in space seems remote, it is not without precedent. A 1962 detonation of a nuclear warhead in Low Earth Orbit by the then US Atomic Energy Commission and Defense Atomic Support Agency resulted in the generation of a significant electromagnetic pulse, the creation of a temporary radiation belt, damage to one third of all satellites in orbit at the time (17), and the subsequent destruction of the British Ariel-1 satellite and NASA’s Telstar-1. This test, named Starfish Prime, was carried out as part of a wider operation titled Operation Fishbowl.</p> <p>Modern satellites are already hardened to some extent against the effects of radiation, as necessitated by the hostile operating environment of space and such hardening renders them more resilient than the satellites of the 1960s. However, the potential yield of modern nuclear weapons far exceeds the estimated 1.4Mt of the Starfish Prime test and thus the potential susceptibility of current space assets to in-space nuclear detonations remains.</p> <p>Additionally, the ejection of a large volume of high energy electrons – beta particles – into the upper atmosphere has the potential to significantly disrupt satellite operations, and any signals that reply on propagation through the ionosphere, such as GPS and high frequency (HF) communications systems.</p> <p>Nevertheless, due to the significant cost and capabilities required to successfully detonate a nuclear warhead in space, and the overt nature of this action in contrast to numerous possible sub-threshold activities, this threat is considered unlikely.</p>			<ul style="list-style-type: none">• Nation-states				
			Related Failure Modes				
			<ul style="list-style-type: none">• FM-001 Physical Destruction• FM-002 Physical Damage• FM-003 Loss of communication• FM-005 Downlink not received• FM-008 Launch vehicle failure				
			Most susceptible segments				
			<ul style="list-style-type: none">• Space• Link				
			Selected Incidents				
			<ul style="list-style-type: none">• 1962 Starfish Prime test (18)				

6.2 Electromagnetic threats


6.2.1 Uplink jamming

	E-001	Uplink jamming	Likelihood				
			1	2	3	4	5
The use of radio frequency energy to interfere with or jam the communications to satellites							
Analysis			Threat Actors				
<p>Uplink jamming involves the generation of intrusive signal noise at the same frequency as the targeted uplink signal from the ground station to the satellite. The jammer must be able to generate a signal at least as powerful as the uplink it is aiming to disrupt, and successful uplink jamming can prevent the command and control of a satellite by the operators.</p> <p>As with all jamming techniques, the jammer must be placed within the field of view of the targeted receiver. In the case of uplink jamming, as the targeted antenna is on the spacecraft, the jammer must be positioned within the vicinity of the ground station from which the satellite receives its commands. This does mean that in contrast to downlink jamming, the uplink jammer does not need to be positioned above the ground station, which could therefore make it an accessible choice to malignant actors. However, as the strength of the jamming signal needs to match that of the ground station, this may require the acquisition of more significant equipment.</p> <p>As uplink jamming can prevent the command and control of the spacecraft, it has the potential to have a global impact on the mission or operation, in contrast to downlink jamming where the effects felt are more local. Additionally, increasing satellite autonomy may limit the impact of uplink jamming, as the mission or operation progresses as planned with limited intervention from ground controllers. Due to the relative ease with which uplink jamming equipment can be obtained, the likelihood of this threat is considered highly likely.</p>			<ul style="list-style-type: none">• Nation-states• Idealogues• Cybercriminals• Thrill seekers/Trolls				
			Related Failure Modes				
			<ul style="list-style-type: none">• FM-003 Loss of communication• FM-004 Payload Failure• FM-006 Propulsion Failure• FM-007 Deployable Appendage Failure• FM-009 Data Processing Error				
			Most susceptible segments				
			<ul style="list-style-type: none">• Link				
			Selected Incidents				
			<p>It is not always clear which method of jamming has been employed and therefore some may be examples of uplink or downlink jamming:</p> <ul style="list-style-type: none">• 2022 Russian jamming of GPS in Ukraine (19)				

6.2.2 Downlink jamming


	E-002	Downlink jamming	Likelihood				
			1	2	3	4	5
The use of radio frequency energy to interfere with or jam the communications from satellites.							
Analysis			Threat Actors				
<p>Downlink jamming involves the generation of intrusive signal noise at the same frequency as the targeted downlink signal from the satellite. In contrast to uplink jamming, which requires the generation of a signal at least as powerful as the targeted transmitter, downlink jamming requires the signal strength to only be as powerful as the received downlink. This results in a relatively simple and accessible form of interference for malign actors.</p> <p>The likelihood of effective downlink jamming can be reduced through the use of directional antennas pointed at the sky, since the jammer must be placed above the target receiver. Whilst this may limit the effectiveness of the most rudimentary jamming activities, which may consist solely of a jammer located in a vehicle or upon a person, there is still susceptibility to air-or space-based jammers.</p> <p>The jammer must also be within the field of view of the target antennae, increasing the risk to omnidirectional antennas, often in use for GPS applications, which have a wider field of view.</p> <p>A jamming attack is usually relatively short-lived, as it is only active for as long as the jammer is in place, whilst its effects do not usually persist beyond the end of the jamming incident. In contrast to uplink jamming, the effects of downlink jamming events are usually local, affecting only the ground station or antenna whose field of view is infiltrated by the jammer.</p> <p>Nevertheless, for the duration of the event, the targeted mission or operation may be significantly disrupted or degraded. It is this potential to disrupt operations for a low cost with relatively little expertise that makes downlink jamming an expected threat, and one that is already encountered on a near-daily basis.</p>			<ul style="list-style-type: none">• Nation-states• Idealogues• Cybercriminals• Thrill seekers/Trolls				
			Related Failure Modes				
			<ul style="list-style-type: none">• FM-003 Loss of communication• FM-005 Downlink not received• FM-009 Data Processing Error				
			Most susceptible segments				
			<ul style="list-style-type: none">• Link				
			Selected Incidents				
			<ul style="list-style-type: none">• 2009 Iranian state jamming of BBC Persia broadcast feed (20)• 2022 Russian jamming of GPS in Ukraine (19)				

6.2.3 Spoofing


	E-003	Spoofing	Likelihood				
			1	2	3	4	5
Alteration and retransmission of signals to potentially issue false commands or otherwise deceive systems.							
Analysis			Threat Actors <ul style="list-style-type: none">• Nation-states• Idealogues• Cybercriminals• Thrill seekers/Trolls				
<p>The effects of a spoofing attack may extend beyond the mission itself and into its applications downstream. Spoofing of GPS signals by an unknown attacker in the Iran-Iraq region in 2023 led to the failure of navigational systems onboard aircraft, resulting in divergences from filed flight paths and in some cases, accidental near-entry into Iranian airspace (21).</p> <p>Some forms of spoofing do not require the breaking of encryption protocols protecting the signal. A technique known as ‘meaconing’ rebroadcasts an authentic signal on a time delay, which can prevent the spoofing attack being discovered whilst corrupting or confusing the target with inaccurate data.</p> <p>As with downlink jamming, GPS systems often present a popular target due to the wider field of view of their omnidirectional antennas. The technology required to spoof satellite signals is commercially available and relatively inexpensive which makes their continued hostile use against space assets highly likely.</p>			Related Failure Modes <ul style="list-style-type: none">• FM-003 Loss of communication• FM-004 Payload Failure• FM-005 Downlink not received• FM-006 Propulsion Failure• FM-007 Deployable Appendage Failure• FM-009 Data Processing Error				
			Most susceptible segments <ul style="list-style-type: none">• Link• Ground				
			Selected Incidents <ul style="list-style-type: none">• 2023 GPS spoofing incidents (21)				

6.3 Cyber threats


6.3.1 Data interception or monitoring

	C-001	Data interception or monitoring	Likelihood				
			1	2	3	4	5
The use of software and network techniques to intercept, monitor, or otherwise gain unauthorised access to mission data.							
Analysis			Threat Actors <ul style="list-style-type: none">• Nation-states• Idealogues• Cybercriminals• Thrill seekers/Trolls• Insiders/Competitors				
<p>Data interception or monitoring is a largely passive attack, which may not cause any collateral damage and therefore may go undetected for a significant period of time.</p> <p>The end goal of this kind of attack is usually to conduct some form of espionage, to monitor data traffic patterns or intercept the data itself and gather intelligence that may be used to inform a future attack or develop some kind of counterspace capability. As with all cyber threats, attribution may be difficult as threat actors utilise various methods to conceal their identify, using hijacked servers, private networks, or the employment of private groups, individuals, or other third parties to carry out the attack on their behalf.</p> <p>This threat may have some crossover with non-destructive co-orbital capabilities (P-002), as a hostile satellite may be manoeuvred to shadow a target or otherwise position itself to interrupt or intercept signals sent to and from the target.</p> <p>The barrier to entry for posing this kind of threat is relatively low, and as with many electromagnetic or cyber threats, the equipment required is commercially available and inexpensive. In 2009, video signals sent via satellite from US surveillance aircraft were intercepted and decoded by Iraqi insurgents (22). This was made possible due to the signals being unencrypted. Nevertheless, the likelihood of this threat being deployed again is considered to be high.</p>			Related Failure Modes <ul style="list-style-type: none">• FM-003 Loss of communication• FM-005 Downlink not received• FM-009 Data Processing Error				
			Most susceptible segments <ul style="list-style-type: none">• Link• Ground				
			Selected Incidents <ul style="list-style-type: none">• 2009 interception of US surveillance video signals (22)				


6.3.2 Data corruption

	C-002	Data corruption	Likelihood				
			1	2	3	4	5
The use of software and network techniques to manipulate, corrupt, or destroy data, preventing or limiting its operational usefulness.							
Analysis			Threat Actors				
<p>Similar to data interception or monitoring, a data corruption attack can be difficult to detect and attribute. In contrast to the passive nature of data interception, data corruption can result in the alteration of authentic data to display false information which may compromise the integrity and reliability of the mission or operation.</p> <p>Whilst there are no public examples of hostile data corruption attacks being carried out against allied space capabilities, an Anonymous-linked hacking collective claimed to have accessed and deleted files after breaching servers of the Russian space agency Roscosmos.</p> <p>Additionally, considerable risk remains of inadvertent data corruption resulting from background radiation or space weather events. Advancements in semiconductor technologies and the resulting reduction in semiconductor size can lower the charge required to change their state, which if left uncorrected could lead to erroneous data being transmitted.</p>			<ul style="list-style-type: none">• Nation-states• Idealogues• Cybercriminals• Thrill seekers/Trolls• Insiders/Competitors				
			Related Failure Modes				
			<ul style="list-style-type: none">• FM-003 Loss of communication• FM-005 Downlink not received• FM-009 Data Processing Error				
			Most susceptible segments				
			<ul style="list-style-type: none">• Link• Ground				
			Selected Incidents				
			<ul style="list-style-type: none">• 2022 Roscosmos breach (5)				

6.3.3 Seizure of control

	C-003	Seizure of control	Likelihood				
			1	2	3	4	5
The use of software and network techniques to gain unauthorised access to satellite or mission assets, rendering them unable to be controlled by legitimate users.							
Analysis			Threat Actors				
<p>A seizure of control can result in irreversible damage to a satellite or space asset if the threat actor is able to gain sufficient control to execute unrecoverable commands.</p> <p>Similarly difficult to attribute but significantly more impactful than data interception or corruption, the attack may not go unnoticed but may be impossible to stop. A seizure of control could lead to the realisation of any of the identified failure modes depending on the intent of the threat actor, their ability to remain undetected for as long as possible, and seizure of a sufficient level of control.</p> <p>A 2011 report to the US Congress from the US-China Economic and Security Review Commission cited two examples of cyber-attacks resulting in a seizure of control. In these instances, control NASA's Terra EOS satellite was seized twice by attackers for 2 and 9 minutes respectively. In this case, no commands were executed, and control was recovered.</p> <p>In 2023, as part of a challenge set by the European Space Agency, a team of cybersecurity experts from Thales Alenia Space successfully took control of a nanosatellite, accessed its onboard system, and introduced malicious code to corrupt and compromise data sent back to Earth (23). Whilst this activity will serve to increase defences against a real attack of this kind, its likelihood nonetheless remains high as malicious actors increasingly look to the cyber domain as a primary means of attack.</p>			<ul style="list-style-type: none">• Nation-states• Idealogues• Cybercriminals• Thrill seekers/Trolls• Insiders/Competitors				
			Related Failure Modes				
			<ul style="list-style-type: none">• FM-001 Physical Destruction• FM-002 Physical Damage• FM-003 Loss of communication• FM-004 Payload Failure• FM-005 Downlink not received• FM-006 Propulsion Failure• FM-007 Deployable Appendage Failure• FM-008 Launch vehicle failure				
			Most susceptible segments				
			<ul style="list-style-type: none">• Link• Ground				
			Selected Incidents				
			<ul style="list-style-type: none">• 2008 attacks against NASA Terra EOS satellite (24)• 2023 ESA/Thales demo (23)				

6.3.4 Supply chain compromise

	C-004	Supply chain compromise	Likelihood				
			1	2	3	4	5
The use of counterfeit microelectronics or the insertion of malware or hidden back doors into components.							
Analysis			Threat Actors				
<p>The complexity in the design and manufacture of space systems, coupled with the need for highly specialised and hardened components, means that long and almost always international supply chains are required to meet demand.</p> <p>Even with rigorous quality controls in place, maintaining close oversight of each and every component, especially more generic ones often found in electrical systems is a formidable undertaking.</p> <p>Therefore, compromising the supply chain, either through malware and other software exploits, or the use of counterfeit or compromised hardware, presents a likely threat vector for deliberate disruption or damage to space capabilities.</p> <p>This threat can be mitigated to varying degrees by diversifying the supply chain, offering fewer opportunities for a compromised supplier to make significant modifications to components, by attempting to bring in-house as much of the design and manufacture of critical components as possible, or by taking an extremely thorough approach to the testing and inspection of components and subsystems.</p>			<ul style="list-style-type: none">• Nation-states• Cybercriminals• Insiders/Competitors				
			Related Failure Modes				
			<ul style="list-style-type: none">• FM-002 Physical Damage• FM-003 Loss of communication• FM-004 Payload Failure• FM-005 Downlink not received• FM-006 Propulsion Failure• FM-007 Deployable Appendage Failure• FM-009 Data Processing Error				
			Most susceptible segments				
			<ul style="list-style-type: none">• Service• Launch• Space				
			Selected Incidents				
			<ul style="list-style-type: none">• Five Eyes security concerns around Huawei 5G involvement (25)				

7 Analysis

7.1 Threats

Electromagnetic and cyber threats have a higher likelihood of occurrence than physical threats

This report found that in general, electromagnetic or cyber threats present a higher likelihood of occurrence than physical threats. This is largely due to the increased sophistication required to carry out a physical threat, and the prohibitive cost of required equipment which for the most part limits this kind of action to hostile nation-states. Additionally, the majority of physical threats would constitute action above the threshold of armed conflict and would likely result in significant military, economic, and political consequences for the aggressor.

Electromagnetic and cyber threats meanwhile can be accomplished using far more rudimentary technology, requiring a lower level of expertise, planning, and funding. Furthermore, the nature of many electromagnetic and cyber threats can make attribution difficult or in some cases impossible, allowing for more frequent sub-threshold activity amongst a wider range of potential threat actors.

Threat ID	Threat Category	Threat Title	Likelihood
E-002	Electromagnetic	Downlink jamming	5
E-001	Electromagnetic	Uplink jamming	4
E-003	Electromagnetic	Spoofing	4
C-001	Cyber	Data interception or monitoring	4
C-004	Cyber	Supply chain compromise	4
C-002	Cyber	Data corruption	3
C-003	Cyber	Seizure of control	3
P-002	Physical	Co-orbital	3
P-001	Physical	Direct Ascent ASAT	2
P-003	Physical	Directed Energy	2
P-004	Physical	Ground station incursion or attack	2
P-005	Physical	In-space nuclear detonation	1

Figure 7-1 - Identified threats, sorted by likelihood

7.2 Failure modes

Failure modes that most likely result in the total loss of the spacecraft and/or ability to complete the mission or operation naturally have the highest impact

The three highest scoring failure modes would or most likely would result in the premature termination of the mission or operation. The range of potential impacts for each failure mode is significant and will depend on the severity of the threat as well as the duration of the failure event.

Failure Mode ID	Failure Mode Title	Impact
FM-001	Physical Destruction	5
FM-008	Launch Vehicle Failure	5
FM-004	Payload Failure	5
FM-002	Physical Damage	4
FM-007	Deployable Appendage Failure	4
FM-003	Loss of communications	3
FM-005	Downlink not received	3
FM-006	Propulsion Failure	3
FM-009	Data Processing Error	2

Figure 7-2 - Identified failure modes, sorted by impact

It is rare that one failure mode will exist in isolation, and there may be considerable overlap between the modes

The nine failure modes identified in this analysis were selected to provide a comprehensive but high-level summary of the possible ways in which a space mission or operation could fail. A more detailed FMECA working at the component level may succeed in decoupling each failure mode from any other, however this is beyond the remit for this report.

As a result, although each of the identified failure modes is distinct in some way, overlaps between them are inevitable. Where identified, these overlaps are discussed in Section 5 but by way of an example, a deployable appendage failure may starve the propulsion system of fuel and result in propulsion failure. Similarly, a launch vehicle failure may lead to the physical destruction of the spacecraft it is carrying. These overlaps where identified have formed part of the impact assessment and resulting impact score.

Impact assessment is intrinsically linked to the threat vector

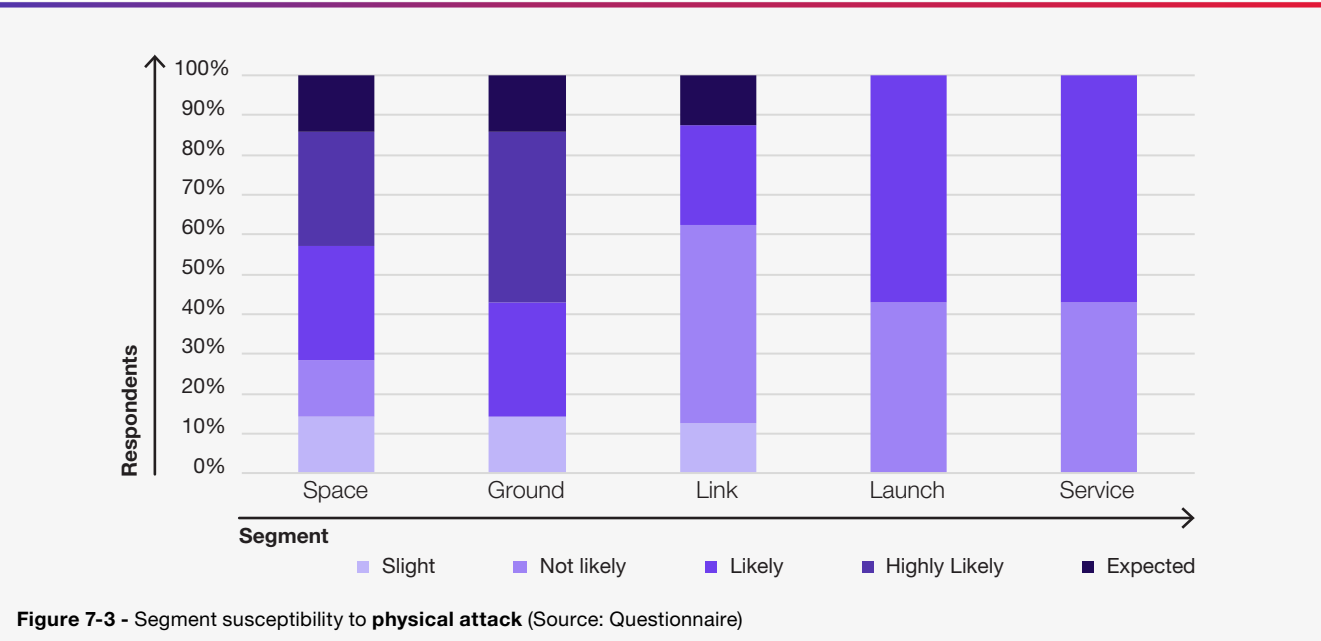
Assessing the impact of any given failure mode without consideration of the events leading up to it is difficult. If taking the worst-case scenario for each failure mode, it would not be unreasonable to score each with the maximum impact as an argument could be made that given sufficient duration any of the above failure modes could result in the eventual total loss of the mission or operation. However, taking such an approach would provide little utility in identifying key areas for the deployment of controls and mitigations. Instead, the impact assessment carried out in this analysis has considers the most likely impact for each failure mode, taking into account the likelihood of the threats that have been identified and linked to them.

The table in Appendix A and corresponding criticality heat map in Appendix B provide some distinction between the overall criticality of each failure mode depending on the related threat.

7.3 Space segment analysis

The link segment is the most vulnerable overall, and most susceptible to electromagnetic and cyber attack

The questionnaire issued as part of this analysis asked, “For each segment, what would you consider to be its susceptibility to physical/electromagnetic/cyber attack?”



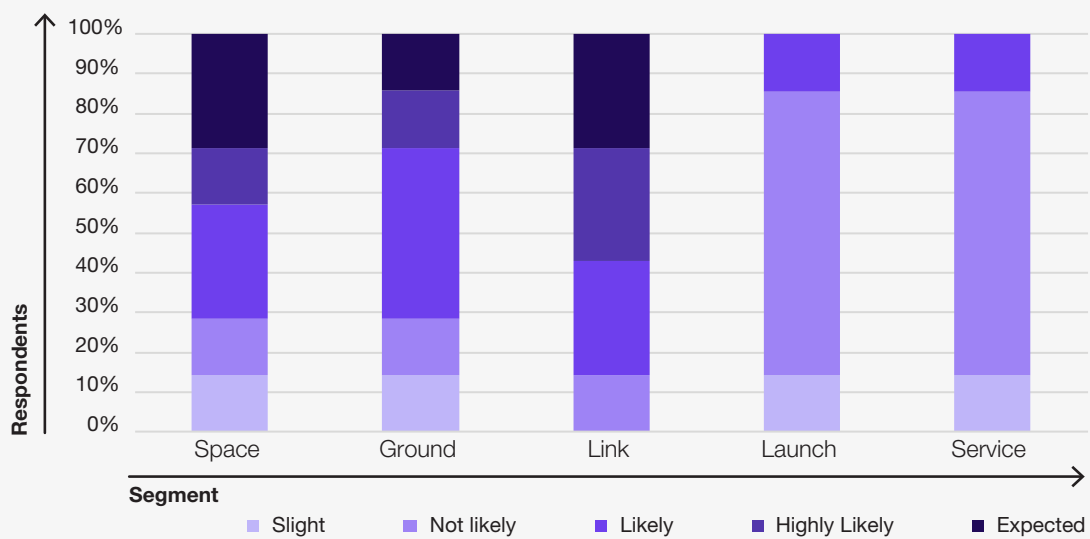


Figure 7-4 - Segment susceptibility to **electromagnetic attack** (Source: Questionnaire)

The questionnaire results showed that the link segment is considered to be the most susceptible to both cyber and electromagnetic attacks which supports the analysis in Section 6, where more potential threats are attributed to the link segment than any other. As discussed in Section 7.1, electromagnetic and cyber threats are considered more likely than physical attacks, contributing to the overall vulnerability of the link segment.

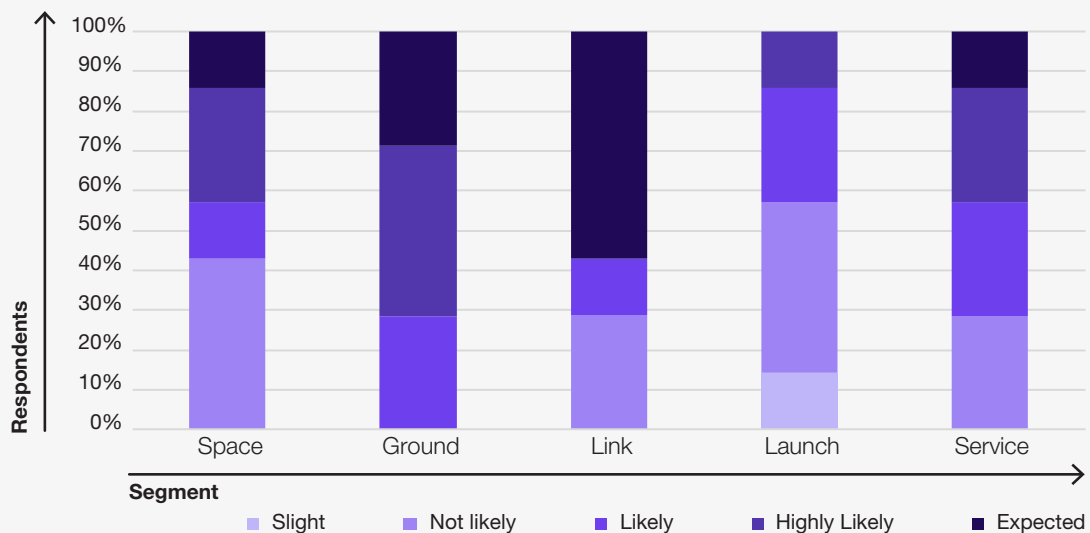


Figure 7-5 - Segment susceptibility to **cyber attack** (Source: Questionnaire)

Whilst threats against launch service segments are still likely, they are considered to be the least susceptible to attack

The majority of the threats identified and analysed in this report target assets in the space, ground, and link segments. A select few may target the launch and service segments but largely these are not considered to be as vulnerable. This is supported by the results of the questionnaire, with only cyber attacks noted as being highly likely or expected in either segment. This may be due to these segments possessing fewer assets of interest to potential threat actors, the relatively small duration of mission or operation time spent in the launch segment, or the breadth of the service segment which may include other systems linked to third parties with additional levels of security. Furthermore, the relative ease with which a threat actor could impact the link segment, perhaps through jamming, versus a complex cyber attack on third party service systems for the same result, may influence a threat actor’s decision to target one segment over another

7.4 Comparisons with the National Risk Register

The perceived level of risk in industry is consistent with the National Risk Register

The questionnaire issued as part of this analysis asked “Overall, what would you perceive to be the likelihood and impact of deliberate disruption of UK space systems and space-based services?”

Score	Likelihood	Impact
1	<0.2%	“Minor”
2	0.2-1%	“Limited”
3	1-5%	“Moderate”
4	5-25%	“Significant”
5	>25%	“Catastrophic”

Figure 7-6 - National Risk Register scoring criteria

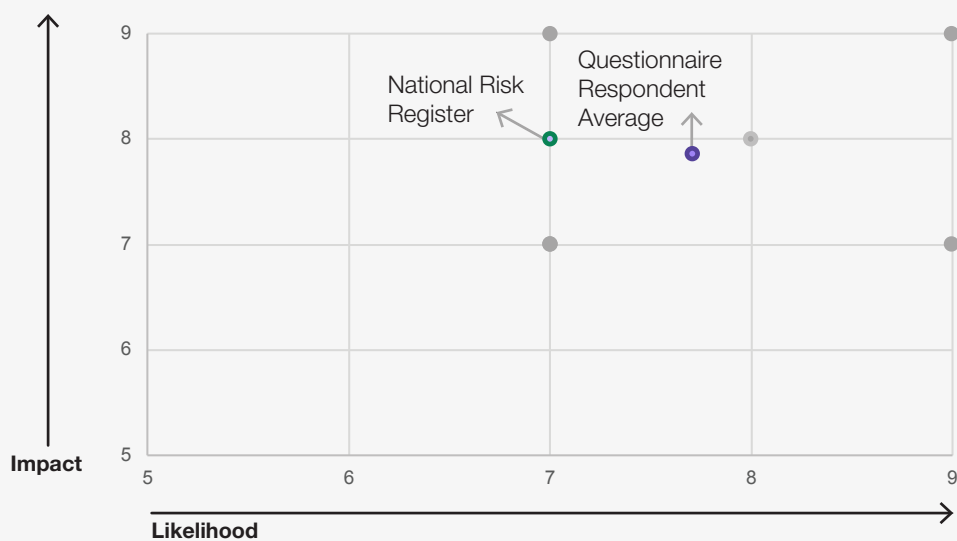


Figure 7-7 - Likelihood and Impact comparison with the National Risk Register

The response options for this question mirrored the criteria used in the National Risk Register (Figure 7 6) to enable a clear comparison of results. It found that, broadly, respondents agreed with the assessment of likelihood and impact stated in the register. It should also be noted that no respondents considered the likelihood of this risk occurring to be lower than stated in the register, whilst some did consider its impact to be 'Moderate' rather than 'Significant'.

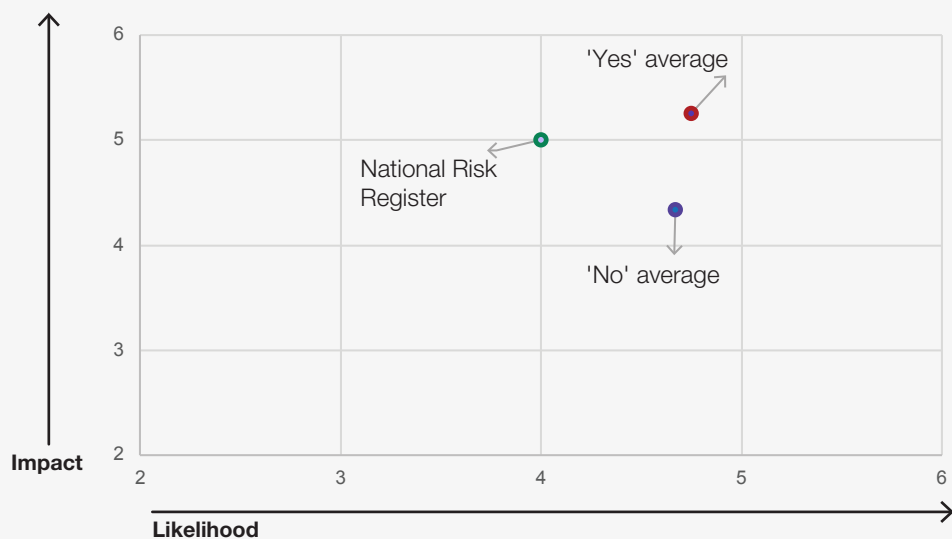


Figure 7-8 - Difference in perceived likelihood and impact based on organisational focus

Respondents representing organisations that own, design, manufacture, operate, or support in-orbit assets perceive a higher impact level than those that do not

57% of the organisations responding to the questionnaire indicated that they own, design, manufacture, operate or support in-orbit assets.

Respondents from these organisations on average ('Yes' average) scored their perceived impact of deliberate disruption of UK space systems and space-based services as higher than those representing organisations that do not own, design, manufacture, operate or support in-orbit assets ('No' average). Perceived likelihood was roughly equal across both groups.

The National Risk Register's reasonable worst-case scenario assumes an attack by a hostile state or proxy, but non-state actors still pose a significant threat

Of the twelve threats identified and analysed in this report, all could reasonably be attributed to nation-state threat actors, or to proxies working in the interests of a nation-state. For all physical threats with the exception of a ground station incursion or attack, it is reasonable to expect that only nation-states or their proxies would possess the means to acquire the advanced and prohibitively expensive capabilities required to pose the threat. However, as this analysis has shown, the relative ease with which electromagnetic and cyber threats can be carried out due to relatively inexpensive components and a lower technological barrier to entry leaves UK space systems and space-based services vulnerable to attacks from other non-state threat actors.

Nevertheless, the most likely threat vector would appear to be a hostile nation-state, utilising sub-threshold electromagnetic or cyber methods to disrupt or degrade UK space systems and services.

8 Closing comments and next steps

This report is the summary of a high-level analysis carried out into the potential threats and resulting failure modes that may contribute to the deliberate disruption of UK space systems and space-based services. It does not constitute a full threat assessment or risk analysis and does not fully cover all possible permutations and scenarios.

Consequently, there are some considerations that are not made in this report that should feed into any subsequent work.

- This report does not make distinction between orbital regimes. It has been noted that whilst the likelihood of disruption to or destruction of assets in lower orbits may be higher, the impacts may be reduced due to the increased redundancy offered by other assets in constellations.
- As mentioned in the previous section, the high-level nature of the identified failure modes gives rise to considerable overlap. A more detailed analysis should aim to decouple failure modes as much as reasonably possible.
- Each failure mode has a general impact score, but a more detailed analysis may wish to assign variable impact score depending on the nature of the threat that has given rise to the failure mode. This should take into account effects on the ability to continue the mission or operation, the duration of the effects, and the risk to life of personnel in orbit or on the ground, as well as damage to the spacecraft.
- This report does not consider the downstream impacts of each failure mode, beyond the impact to the spacecraft and its mission. Every satellite has a purpose, which may be military, civilian, or dual-use. The knock-on effect of each failure mode on this purpose, the wider space ecosystem, and its stakeholders should be considered in a future analysis.
- The questionnaire used in this analysis was disseminated by various channels to UK space industry stakeholders. The analysis presented in this report is true to its responses, however a much larger sample size and the inclusion of respondents from across all of the UK space sector (including military and academia) is required to draw more accurate conclusions and shape the preparation of suitable mitigations and controls to protect UK space assets and services.
- Additionally, this report makes no attempts to identify existing mitigations or controls or to suggest the implementation of specific measures. Subsequent work should focus on identifying where these mitigations and controls are most necessary.

References

1. [House of Commons Defence Committee. UK Defence and the Indo-Pacific.](#) [Online] 24 October 2023.
2. [National Cyber Security Centre. NCSC Annual Review 2023.](#) [Online] 14 November 2023.
3. [House of Commons Defence Committee. Defence in the Grey Zone.](#) [Online] 18 September 2023.
4. [United Nations Office for Outer Space Affairs. Online Index of Objects Launched into Outer Space.](#) [Online] 1 February 2024.
5. [Center for Strategic & International Studies. Space Threat Assessment 2023.](#) [Online] April 2023.
6. [Secure World Foundation. Global Counterspace Capabilities Report.](#) [Online] April 2023.
7. [National Air and Space Administration. Standard for Performing a Failure Mode and Effects Analysis \(FMEA\) and Establishing a Critical Items List.](#) [Online] [Cited: 31 January 2024.]
8. [In-Q-Tel. The Evolution of IQT's Space Framework.](#) [Online] 7 Feb 2021.
9. [National Aeronautics and Space Administration. Study of Spacecraft Deployables Failures.](#) [Online] [Cited: 20 February 2024.]
10. [Scientist, New. First satellite launch from the UK failed due to an 'anomaly'.](#) [Online] 10 January 2023.
11. [Secure World Foundation. List of ASAT Tests in Space.](#) [Online] 30 January 2024.
12. [National Aeronautics and Space Administration. NASA Space Science Data Coordinated Archive.](#) [Online]
13. [US Department of State. Whither Arms Control in Outer Space? Space Threats, Space Hypocrisy, and the Hope of Space Norms.](#) [Online] 6 April 2020.
14. [Time. Exclusive: Strange Russian Spacecraft Shadowing U.S. Spy Satellite, General Says.](#) [Online] 10 February 2020.
15. [Defense Intelligence Agency. 2022 Challenges to Security in Space.](#) [Online] March 2022.
16. Air Command and Staff College, and Space Research Electives Seminars. AU-18 Space Primer. s.l. : Air University Press, 2009.
17. Edward E. Conrad, Gerald A. Gurtman, Glen Kweder, Myron J. Mandell, and Willard W. White. Collateral Damage to Satellites from an EMP Attack. Ft Belvoir, VA : Defense Threat Reduction Agency, 2010.
18. [Stassinopoulos, E.G. The STARFISH Exo-atmospheric, High-altitude Nuclear Weapons Test. NASA.](#) [Online]
19. [Royal United Services Institute. Jamming and Cyber Attacks: How Space is Being Targeted in Ukraine.](#) [Online] 5 April 2022.

20. [British Broadcasting Corporation. BBC Persian television broadcasting despite interference from Iran. BBC Press Office.](#) [Online] 21 December 2009.
21. [Forbes. Someone In the Middle East is Leading Aircraft Astray by Spoofing GPS Signals.](#) [Online] 28 September 2023.
22. [The Guardian. US drones hacked by Iraqi insurgents.](#) [Online] 17 December 2009.
23. [SpaceRef. Thales Seizes Control of ESA Demonstration Satellite in First Cybersecurity Exercise of Its Kind.](#) [Online] 26 April 2023.
24. [US-China Economic and Security Review Commission. 2011 Report to Congress.](#) [Online] November 2011.
25. [National Cyber Security Centre. Summary of the NCSC analysis of May 2020 US sanction.](#) [Online] 14 July 2020.

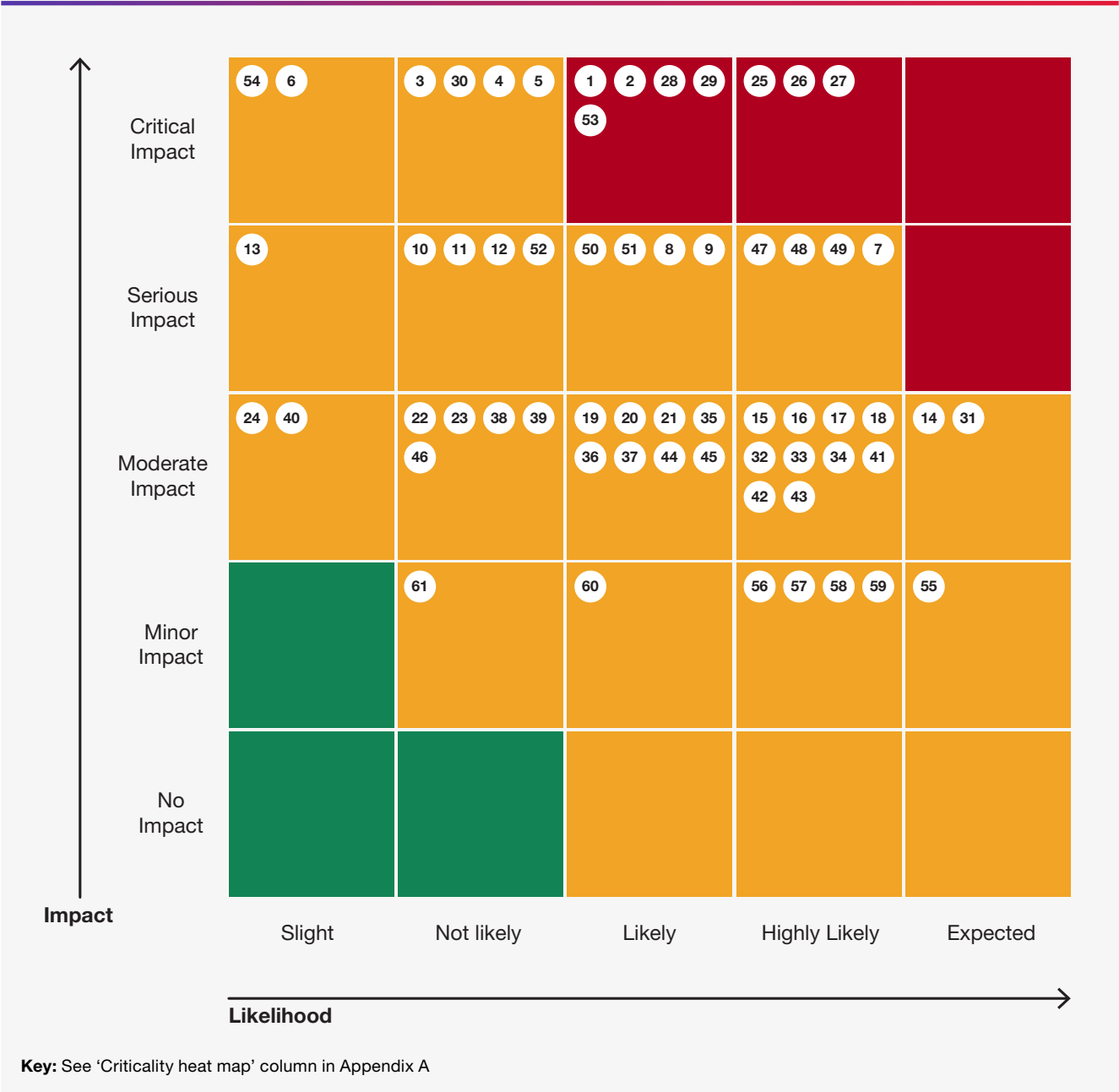
Appendix A - Mapping failure modes to threats (tabular)

Failure Mode	Impact	Threat	Likelihood	Criticality heat map reference
FM-001 Physical Destruction	5 Critical Impact	C-003 Seizure of control	3 – Likely	1
		P-002 Co-orbital	3 – Likely	2
		P-001 Direct Ascent ASAT	2 – Not Likely	3
		P-003 Directed Energy	2 – Not Likely	4
		P-004 Ground station incursion or attack	2 – Not Likely	5
		P-005 In-space nuclear detonation	1 - Slight	6
FM-002 Physical Damage	4 Serious Impact	C-004 Supply chain compromise	4 – Highly Likely	7
		C-003 Seizure of control	3 – Likely	8
		P-002 Co-orbital	3 – Likely	9
		P-001 Direct Ascent ASAT	2 – Not Likely	10
		P-003 Directed Energy	2 – Not Likely	11
		P-004 Ground station incursion or attack	2 – Not Likely	12
		P-005 In-space nuclear detonation	1 - Slight	13
FM-003 Loss of communication	3 Moderate Impact	E-002 Downlink jamming	5 – Expected	14
		E-001 Uplink jamming	4 – Highly Likely	15
		E-003 Spoofing	4 – Highly Likely	16
		C-001 Data interception or monitoring	4 – Highly Likely	17
		C-004 Supply chain compromise	4 – Highly Likely	18
		C-002 Data corruption	3 – Likely	19
		C-003 Seizure of control	3 – Likely	20
		P-002 Co-orbital	3 – Likely	21
		P-003 Directed Energy	2 – Not Likely	22
		P-004 Ground station incursion or attack	2 – Not Likely	23
		P-005 In-space nuclear detonation	1 - Slight	24

Failure Mode	Impact	Threat	Likelihood	Criticality heat map reference
FM-004 Payload Failure	5 Critical Impact	E-001 Uplink jamming	4 – Highly Likely	25
		E-003 Spoofing	4 – Highly Likely	26
		C-004 Supply chain compromise	4 – Highly Likely	27
		C-003 Seizure of control	3 – Likely	28
		P-002 Co-orbital	3 – Likely	29
		P-003 Directed Energy	2 – Not Likely	30
FM-005 Downlink not received	3 Moderate Impact	E-002 Downlink jamming	5 – Expected	31
		E-003 Spoofing	4 – Highly Likely	32
		C-001 Data interception or monitoring	4 – Highly Likely	33
		C-004 Supply chain compromise	4 – Highly Likely	34
		C-002 Data corruption	3 – Likely	35
		C-003 Seizure of control	3 – Likely	36
		P-002 Co-orbital	3 – Likely	37
		P-003 Directed Energy	2 – Not Likely	38
		P-004 Ground station incursion or attack	2 – Not Likely	39
FM-006 Propulsion Failure	3 Moderate Impact	P-005 In-space nuclear detonation	1 - Slight	40
		E-001 Uplink jamming	4 – Highly Likely	41
		E-003 Spoofing	4 – Highly Likely	42
		C-004 Supply chain compromise	4 – Highly Likely	43
		C-003 Seizure of control	3 – Likely	44
		P-002 Co-orbital	3 – Likely	45
FM-007 Deployable Appendage Failure	4 Serious Impact	P-003 Directed Energy	2 – Not Likely	46
		E-001 Uplink jamming	4 – Highly Likely	47
		E-003 Spoofing	4 – Highly Likely	48
		C-004 Supply chain compromise	4 – Highly Likely	49
		C-003 Seizure of control	3 – Likely	50
		P-002 Co-orbital	3 – Likely	51
		P-003 Directed Energy	2 – Not Likely	52

Failure Mode	Impact	Threat	Likelihood	Criticality heat map reference
FM-008 Launch Vehicle Failure	5 Critical Impact	C-003 Seizure of control	3 – Likely	53
		P-005 In-space nuclear detonation	1 - Slight	54
FM-009 Data Processing Error	2 Minor Impact	E-002 Downlink jamming	5 – Expected	55
		E-001 Uplink jamming	4 – Highly Likely	56
		E-003 Spoofing	4 – Highly Likely	57
		C-001 Data interception or monitoring	4 – Highly Likely	58
		C-004 Supply chain compromise	4 – Highly Likely	59
		C-002 Data corruption	3 – Likely	60
		P-004 Ground station incursion or attack	2 – Not Likely	61

Appendix B - Criticality heat map





About CGI

Insights you can act on

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. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

cgi.com/uk/space

© 2025 CGI IT UK Ltd.

