MNE7

Access to the Global Commons

Protecting Access to Space

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUL 2013	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Multinational Experiment 7 Access to Global Commons: Protecting access to space	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
Aim to provide a useful guide for senior leaders and managers, both civilian and military, in government and commercial organisations. Some readers will have considerable experience of space-related issues, while others may have none. Chapter 1 provides the foundation while in Chapter 2 we propose a framework for protecting access to space, describing the potential consequences of disruption or denial of space capabilities and how to mitigate their loss.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**37**	

Preface

Under the lead of the US Joint Staff J7 Joint Coalition Warfare, the Multinational Experiment (MNE) series has been running since 2001. Each campaign is designed to examine a topical defence and security issue in a comprehensive and unclassified environment. The MNE 7 community involved 17 nations and NATO, with participants from the military, academia, industry, and other entities.

The MNE 7 campaign started in January 2011 and concluded in December 2012. Our aim was to develop solutions to address the challenges of *Access to the Global Commons*. For campaign purposes, we considered the global commons to be:

> *Areas that are potentially accessible to any, and all actors, be they states, non-states, or individuals. Although this term is generally applied only to ungoverned access pathways between sovereign spaces, or those areas that are outside the jurisdiction of any nation, Multinational Experiment 7 also addressed areas that fall under some degree of national sovereignty when they are relevant to ensuring access to, and freedom of action within, the global commons*.

For MNE 7, a problem was defined:

> *Nations and organisations require concepts and capabilities for anticipating, deterring, preventing, protecting against, and responding to, a disruption or a denial of access to the global commons domains (air, maritime, space and cyber). It also ensures freedom of action within them, while taking into account their interrelationships*.

We identified three domain-focused strands of work: cyber; maritime; and space, as well as an inter-domain one. The space domain strand addressed three objectives:

- Identifying dependencies on, threats to, and vulnerabilities of, space capabilities.

- Identifying mechanisms to deter, coerce, or influence actors in space.
- Developing proposals for mitigation.

Canada, Poland, South Korea, Sweden, Switzerland, UK, US and NATO Headquarters Supreme Allied Commander Transformation agreed to contribute to this space domain strand. The UK led the first, NATO HQ SACT the second, and Canada the third. This guide summarises the main outputs of the campaign. Annex A provides a summary of all the products. This guide should be read in conjunction our earlier publication, *Space: Dependencies, Vulnerabilities and Threats*.

Purpose of this guide

We aim to provide a useful guide for senior leaders and managers, both civilian and military, in government and commercial organisations. Some readers will have considerable experience of space-related issues, while others may have none. Chapter 1 provides the foundation while in Chapter 2 we propose a framework for protecting access to space, describing the potential consequences of disruption or denial of space capabilities and how to mitigate their loss.

Structure of this guide

We have structured the guide to provide a logical path to addressing the problem of protecting access to space.

Questions	Answers
Why does access to space need to be protected?	▪ Chapter 1: Space dependencies ▪ Chapter 2: Identifying space dependencies
What could be done to manage actor behaviour in space?	▪ Chapter 2: A process to influence actors in space
What could be done to minimise the effects of disruption or a denial of access to space?	▪ Chapter 2: Space defence ▪ Chapter 2: Collaborative space mitigation

Protecting access to space

Contents

Chapter 1 – Foundation

Section 1 – The space problem

101. We depend on space to enhance and enable a broad range of military, governmental, and commercial capabilities. However, our access to space is vulnerable to hazards and threats. So, we must adopt new strategies to assure necessary space capabilities. These strategies must be proactive, and develop the means to influence, deter, defend and mitigate the consequences of harmful actions in space.

102. As an environment, space is sensitive to disruption. Human activities pollute space. Examples include:

- clouds of debris from kinetic anti-satellite missiles;
- decommissioned spacecraft;
- items lost during missions; or
- expended rocket boosters.

Space debris is a cause of significant concern since it is persistent, and difficult and expensive to clean up.

103. These issues are compounded by the fact that the capacity of space is finite. There is limited availability of useful orbits and consequently, they are congested. An actor could simply place sufficient debris into orbits to deny their use. Worse still, it is estimated that the density of debris has reached levels where the presence of more debris could result in a chain reaction of collisions, each generating more debris and rendering orbits unusable. A chain reaction of collisions occurring in low earth orbit is also likely to deny access to space as spacecraft would not be able to transit to higher orbits safely.

104. Furthermore, our reliance on space makes it a tempting target for potential actors, who may wish to negate economic or security advantages in other domains by disrupting space-enabled capabilities. A range of options exists to disrupt or deny the space, ground, and communication segments of space systems, thereby degrading space capabilities. Protecting ground and

communication segments falls within the remit of existing publications thus, this guide concentrates on protecting the space segment.

105. The cost of protecting against the range of potential hazards and threats needs a proactive and collaborative approach to increase the resilience of space capabilities. Such an approach must identify measures that should be taken before, during and after a disruption or denial.

Section 2 – Space fundamentals

The boundary of space

106. While various definitions for the boundary of space have been proposed, international law does not define an absolute altitude. In fact, there is no clear natural physical boundary between the atmosphere and space. Beyond 30 km, air density decreases to the point where conventional aviation becomes impossible. Only as altitude increases toward 100 km does atmospheric drag and frictional heating reduce to the point where spacecraft operation becomes practical. Some commentators therefore quote 100 km, known as the Karman Line, as the boundary that marks the start of space. The 70 km gap between conventional aviation and space is sometimes referred to as near-space. In practice, there are few satellites in orbit below 150 km. Figure 1.1 shows the different orbital altitudes.

107. These definitions are important because of the legal implications for space operations. Under international law, aircraft, missiles and rockets flying over a country are considered to be in its national airspace, regardless of their altitude. Even though their altitude may sometimes be less than that achieved by rockets and missiles, there is no consensus whether orbiting spacecraft are considered to be in national airspace. One reason why space may be regarded as a global common is because spacecraft have free access to the space over any country, regardless of national boundaries.

Orbits

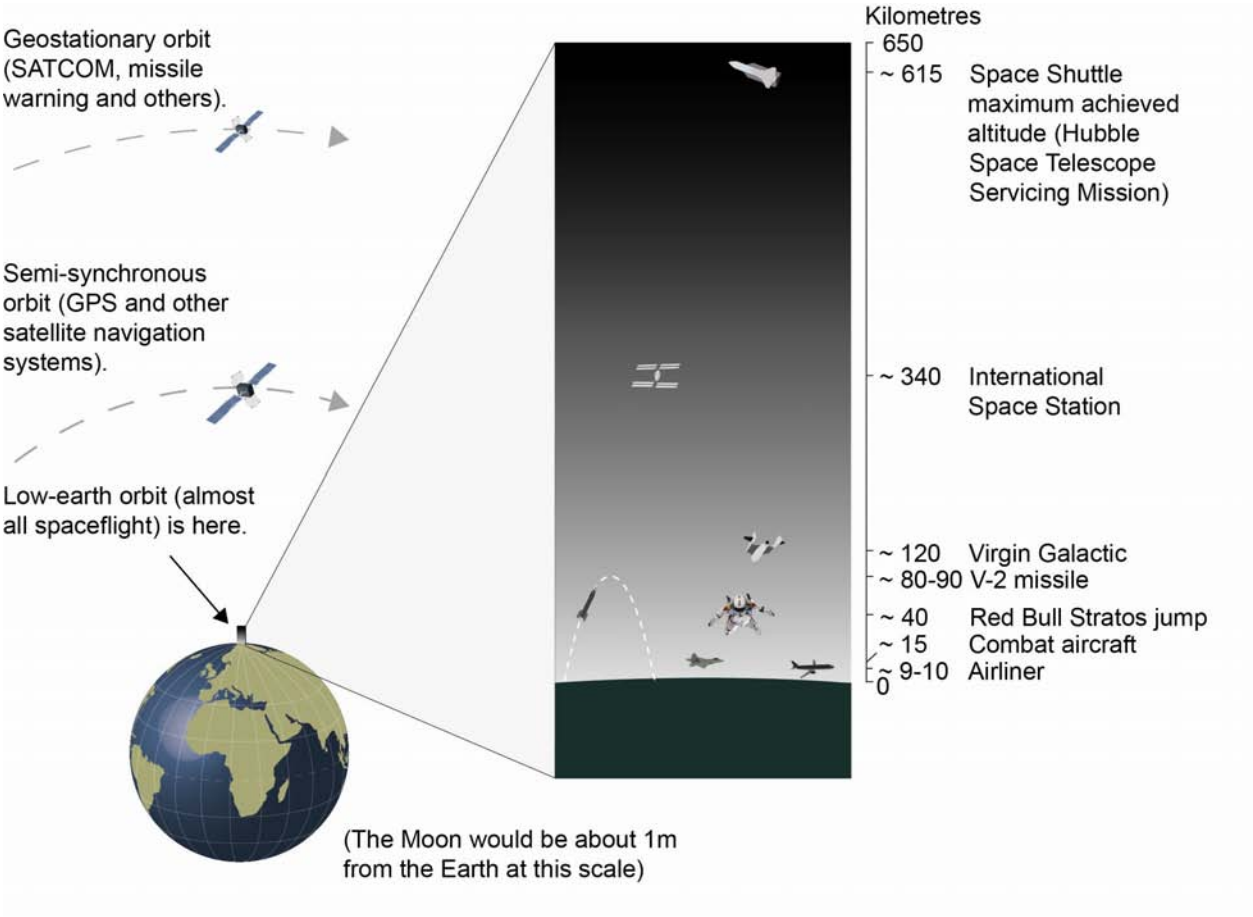

Figure 1.1 – Summary of orbital altitudes to a common scale

108. **Low-earth orbits**. There is no formal definition of low-earth orbit but it is generally considered to have an apogee (the point in an orbit that is farthest from the earth) of no more than 1000 km. At low altitudes, atmospheric drag will limit a spacecraft's life, unless it is boosted periodically into a higher altitude. At an altitude of 320 km, without any boosting, a spacecraft's operational life would be expected to be around one year. This can be increased to around 10 years at an altitude of 800 km. Low-earth orbit is ideal for observation, environmental monitoring and small communications satellites. Manned spacecraft, such as the International Space Station, generally remain below 500 km to prevent the need for heavy shielding to protect the crew from the Van Allen radiation belt.[1] Objects in

[1] The Van Allen radiation belt is composed of two torus-shaped layers of energetic charged particles (plasma) around Earth, held in place by a magnetic field. It is thought that most of the particles that form the belts come from solar wind and other particles of cosmic rays.

low-earth orbit have the advantage that they pass relatively close to the Earth, so they can use less powerful sensors and transmitters, but they will only be in the view of a ground user or station for the short period of time when overhead. For this reason, for some applications, a constellation of several satellites spaced around the same or similar orbits is used to provide continuous coverage. A satellite in circular low-earth orbit with an altitude of 850 km will travel at a speed of 24,600 km per hour, about 7 km per second.

109. **Medium-earth orbits**. Again, there is no formal definition of a medium-earth orbit, but it is considered to include those orbits between low-earth orbit and geostationary orbit. A semi-synchronous orbit is a special case of a medium-earth orbit, which has a nearly circular orbit that repeats an identical ground trace twice each day: hence the term semi-synchronous. The global positioning system satellites use this type of orbit, at an altitude of 20,830 km and speed of 14,330 km per hour.

110. **Geosynchronous and geostationary orbits**. A geosynchronous orbit has a period equal to that of the Earth's rotation. Geosynchronous satellites will have an altitude of approximately 36,000 km. Varying the incline of the orbit produces ground traces that fluctuate north and south of the equator in a figure-of-eight pattern. The larger the incline, the larger the figure-of-eight. Some kinds of communications, weather and surveillance or warning satellites use geosynchronous orbits. A geostationary orbit is a special kind of geosynchronous orbit where the incline is zero and the orbital plane coincides with the Earth's equatorial plane. To an observer on the Earth, the satellite appears to be stationary overhead. The most significant advantage with this orbit is that the satellite provides continuous coverage of specific areas of the Earth and ground antennas do not need to track the satellite. Geostationary orbits are used extensively for communications, weather and some earth-observation activities. However, coverage only extends to about 70° north and south of the equator, so alternative orbits are required if coverage is needed in the polar regions. In geostationary orbits, a satellite will have an altitude of 37,160 km and travel at 11,120 km per hour.

111. **Other orbits**. Orbits designed for specific purposes can be achieved. For example, a satellite in a highly elliptical orbit, such as the Molniya orbit, (semi-synchronous) spends 11.7 hours of its 12-hour period in the northern hemisphere. This makes the Molniya orbit well suited for communications

satellites that are intended to provide coverage in the extreme north, where access to geostationary orbits is impractical.

Space capability

112. A simple model of any space capability has three segments, as shown at Figure 1.2. The space segment lies outside the Earth's atmosphere and consists of spacecraft in various orbits. The communications segment links the space and ground segments. Finally, there is the ground segment which:

- receives products from space;
- controls spacecraft; and
- launches or recovers spacecraft.

113. Disruption to any segment has the potential to deny the use of space capabilities.

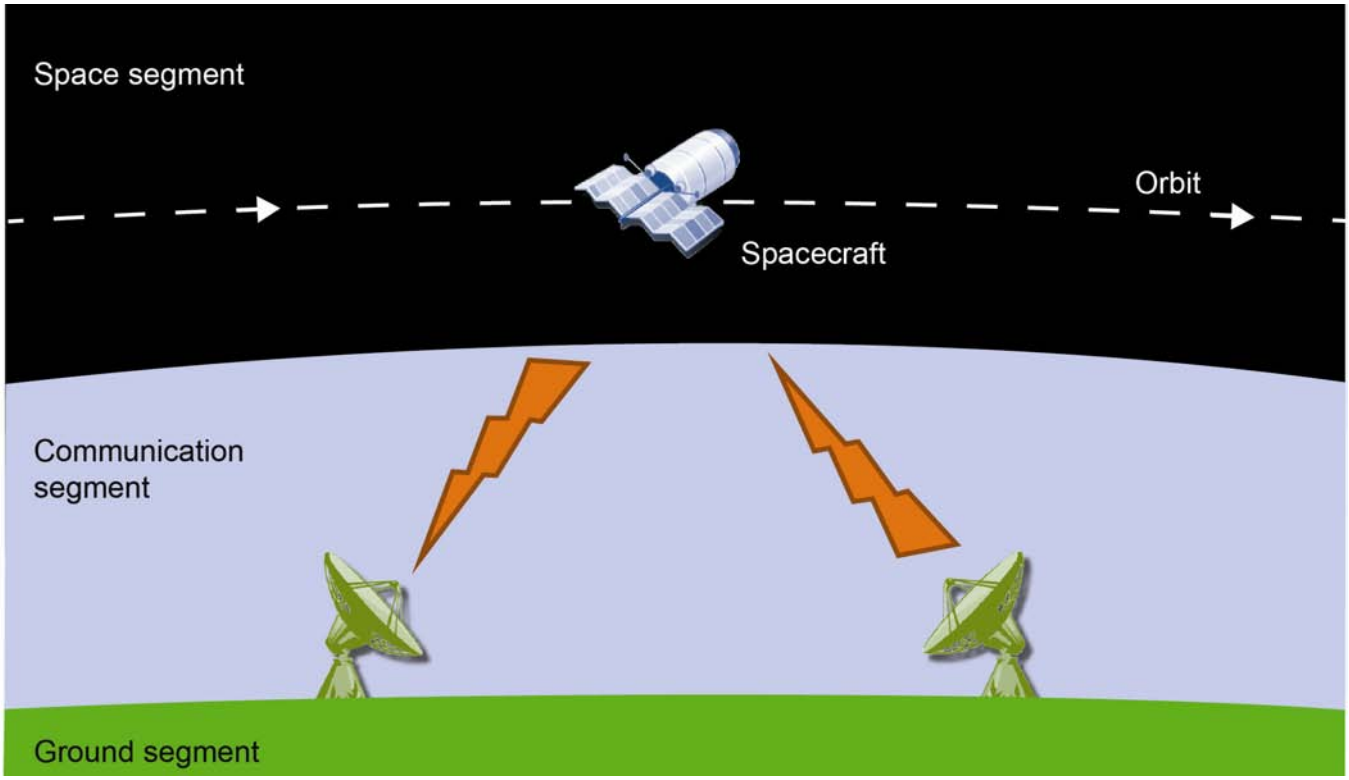

Figure 1.2 – Space capability segments

114. **Space pillars**. We use four **space pillars** to describe the types of capabilities that space can provide:

a. **Position, navigation and timing**. The timing and data signals received from different satellites in a global navigation system can be combined to determine a user's position (including elevation), time or speed with precision.

b. **Satellite communications**. Space provides beyond line-of-sight communications of significantly higher quality and capacity than terrestrial radio systems. Such space capabilities may be military, or increasingly, civilian.

c. **Intelligence, surveillance and reconnaissance**. Surveillance of earth from space provides unique intelligence capabilities. These include unrestricted global access to overhead observations using various types of sensors. Space-derived intelligence, surveillance, and reconnaissance may be used for wide-ranging applications, from direct support to military operations through to environmental monitoring, disaster relief and urban planning. Consequently, this space capability is inherently dual-use and military, governmental and commercial satellites provide free products and services.

d. **Space situational awareness**. Space situational awareness is important to successfully delivering the other three space pillars. It is achieved by integrating information from different types of sensors to provide a comprehensive understanding of the space environment, including tracking space objects and monitoring space weather. The most effective level of space situational awareness will be achieved if the necessary information is shared.

Space law

115. Most law relating to space activity is based on international treaties, rather than on customary law or teaching by scholars. The key treaty is the **Outer Space Treaty of 1967**. As of January 2008, 98 nations are parties to the treaty, while a further 27 nations have signed, but not yet ratified. The key provisions of the Outer Space Treaty are listed below.

a. **Weapons of mass destruction**. The treaty prohibits the placing of any weapons of mass destruction, including nuclear warheads, in orbit around the Earth. It does not prohibit the stationing of conventional weapons in orbit, nor does it regulate nuclear weapons that pass through space without achieving orbit.

b. **Other weapons and military activity**. Establishing military bases, the testing of weapons of any kind, or conducting military manoeuvres on the Moon, or any other celestial body, is not allowed. The treaty does not, however, limit such activity in the Earth's orbit.

c. **Sovereignty**. A launching nation maintains the sovereignty and jurisdiction over any activity occurring in a manned spacecraft. A satellite remains the property of its owner.

d. **Peaceful use**. The overarching aim of the treaty is to promote the peaceful use of space for the benefit of all mankind. There is nothing in the treaty, however, that prohibits military activities, such as reconnaissance, missile warning, space surveillance and the use of terrestrial weapons that rely on space capabilities.

116. **Other space-related regulations**. The following examples illustrate some of the more commonly encountered laws and conventions.

a. **Rescue Treaty**. The 1968 Rescue Treaty commits signatories to:

- assist in the rescue of spacecraft personnel where able;
- retrieve space objects outside their territory of origin; and
- ensure the safe return of people and property to their original owners.

b. **Liability Convention**. The Liability Convention makes states liable for damage to people or property caused by their space activities, whether caused in space or on the Earth. It also sets out liability rules.

c. **The Registration Convention**. The Registration Convention established a UN register of space objects. Launching nations must create and maintain a public register of orbital elements for objects they place in orbit. They must also separately notify the UN of such actions. Unfortunately, nations interpret the convention in different ways and the amount of detail registered varies. As with many issues relating to behaviour in space, it is not enforced.

d. **Limited Test Ban Treaty**. This treaty bans nuclear weapons test explosions, or other nuclear explosions, in any environment, including space. Not all spacefaring nations have signed it.

e. **Allocation of geostationary orbits**. Since a geostationary orbit has a fixed view of the Earth, slots above populous areas are particularly valued. By mutual agreement, the International Telecommunications Union (a UN agency) coordinates and controls allocating orbital slots, since the vast majority of geostationary activity relates to communications and wide-area broadcast functions.

Section 3 – Vulnerabilities, hazards and threats

117. This section lists the main vulnerabilities of space capabilities in terms of the hazards and threats that may be encountered. Additional detail is available in Chapter 4 of *Space: Dependencies, Vulnerabilities and Threats*.[2]

Hazards

118. **Space Weather**. Almost all natural hazards in the space segment come from the Sun. Principally, these manifest themselves as increased electromagnetic noise, ionospheric interference or prolonged impact by energetic charged particles. The various phenomena resulting from the Sun's activity are collectively termed *space weather*. Weather in space is caused by changes in solar activity, which results in increased or decreased levels of cosmic rays, solar flares, coronal mass ejections and other natural phenomena.

[2] MNE 7, *Space*: *Dependencies, Vulnerabilities and Threats*, produced by the UK MOD DCDC, available at www.mod.uk/dcdc.

119. The Sun emits a solar wind; a stream of charged atomic particles ejected from its upper atmosphere at high speed. Although the particles are very small, they impact continuously at significant speeds on the sun-facing surfaces of a spacecraft. The effect is cumulative and measurably alters the orbit over time. It can also introduce rotation by generating asymmetric forces on specific parts of the object.

120. Various specific effects associated with solar wind are listed below.

a. Individual charged particles can penetrate and damage electronic circuits, or reduce the reliability of electronic components.

b. The continuous impact of solar particles on the spacecraft's outer surface can cause physical damage.

c. Electrically-charged particles accumulating on the surface of the spacecraft can transfer their charge to the structure. When these discharge, they can cause severe damage, or create spurious signals, which may cause equipment to malfunction.

d. Increased solar activity warms the outer layers of the atmosphere, causing it to expand outwards from the earth. This can affect orbits by increasing drag.

121. **Space debris**. Orbits around Earth have become increasingly cluttered with debris. Much of this is unintentional, such as decommissioned satellites, spent rocket cases that remain in orbit after launching their payload, tools dropped by astronauts, failed components and even tiny flecks of paint. There are several issues caused by orbital debris:

a. **Debris dispersal**. If an object detaches from an orbiting body, no matter what its size, it will initially follow the same orbit, varied only by the event that caused the break up. This means that debris may take weeks, months or even years to separate from its source. Even clouds of objects, created by explosive events, will only slowly disperse once the initial explosion is complete. Depending on altitude and velocity, such objects may remain in a stable orbit for extended periods of tens, or even hundreds, of years.

b. **Collisional cascading**. The preferential use of certain orbits increases the risk of collision by concentrating large numbers of objects in discrete bands. Space is increasingly congested. There are now about 800 active satellites and, as a result of 60 years of operations in space, nearly 21,000 objects larger than 10 cm in the Earth's orbit. There are also an estimated 300,000 items of untracked debris between one cm and 10 cm in size. There are growing fears that as the orbital space around the Earth becomes increasingly cluttered, a future collision may create a runaway chain of events that causes collision after collision, rendering some orbits unusable for centuries. This is known as **collisional cascading** or the Kessler Syndrome.

122. **Frequency fratricide**. The unintentional hazard of frequency fratricide is becoming an increasingly important issue. One of the major difficulties with operating spacecraft is not how close they operate, but rather how the limited numbers of radio-frequency bands on which they rely for operation are allocated. Adjacent spacecraft cannot operate on the same frequency without interference.

Threats

123. Some capabilities designed to affect space are widely available; for example, position, navigation, and timing signal jammers. However, some are limited to a few nations, such as direct ascent anti-satellite systems. General near- and far-term threats include:

- direct attack (kinetic and cyber);
- electronic attack (jamming and spoofing);
- laser blinding; and
- electromagnetic pulse attack.

124. **Direct attack**. Direct attacks include both kinetic and cyber attacks mounted against the space, ground or communication segments. Kinetic attacks launched against spacecraft or orbits through fragments from the detonation of a warhead may be effective. They may lead to the damage of other spacecraft or denial of other orbits, so it may be more productive, and

easier, to target the ground segment. Several companies and nations are proposing or developing systems to service satellites or collect and remove space debris. There is a possibility that these systems could also be used in an anti-satellite role. Cyber attacks could be aimed at our computer systems used to control satellite functions and networks designed to collect, process and disseminate mission data.

125. **Electronic attack**. Ground or space radio frequency jamming equipment can be used to break down the communication segment. Cyber may also be used to spoof space capabilities by modifying data. The effects of electronic attacks mean that targets may be unaware of the attack or believe that they have suffered from system failure. It may also be very difficult to attribute responsibility for electronic attacks.

126. **Laser blinding**. Ground, air or potentially space-based laser systems may be used to target the optical components of reconnaissance satellites. This capability offers the advantage of inflicting temporary or permanent damage, yet does not affect the orbit.

127. **Electromagnetic pulse attack**. These weapons are capable of degrading or destroying ground or space segment electronics. A recent technical report from the US-based Defense Threat Reduction Agency noted that low-earth orbit satellites are at serious risk of collateral damage caused by high-altitude nuclear detonations.

Section 4 – Space dependencies

128. There are many areas in which commercial, government and military activity relies upon access to space-based services. Space provides most nations with critical, and often unique, capabilities that:

- enable agriculture;
- support disaster-relief efforts;
- assist in resource prospecting; and
- enhance the abilities of our forces.

129. Several examples are outlined below. For more detail and additional case studies, refer to *Space: Dependencies, Vulnerabilities and Threats*.

a. **Agriculture**. Growth in the Earth's population requires ever more efficient agricultural methods. Correspondingly, farming processes are increasingly taking advantage of space services. In addition to their use in informing crop location, cultivation and compliance activity, satellites are used to guide modern farm machinery to within a few centimetres of an exact path, thereby improving efficiency and lowering costs of production.

b. **Mineral and oil prospecting**. Mapping and detecting earth resources are reliant upon space-based surveillance systems. Terrestrial techniques may provide an alternative method, but cost more and increase the time taken. Satellite observation is often the only means to detect, in a timely manner, spills or other environmentally damaging consequences of extraction.

c. **Air-delivered weapons**. Many air-delivered weapons rely upon global positioning system input to accurately hit their target. We need such precision to avoid collateral damage and civilian casualties.

Chapter 2 – A framework for protecting access to space

201. To protect our access to space, we propose a three-phase framework.

- **Phase 1 – Before**. This phase identifies and prioritises space dependencies and aims to influence an actor's will to disrupt or deny.
- **Phase 2 – During**. This phase considers a number of defensive measures available to spacecraft when they are being attacked.
- **Phase 3 – After**. This final phase maximises the use of existing space capabilities through mitigation.

Phase 1 (Before) – Identifying space dependencies

Critical national infrastructure

202. When analysing the presence of dependencies, vulnerabilities and threats, it is useful to agree where these factors apply. This gives rise to the **concept of critical national infrastructure** which for our use, describes the facilities, systems, sites and networks necessary for the delivery of the essential services upon which daily life depends. For example, the UK uses nine critical national infrastructure sectors:

- communications;
- emergency services;
- energy;
- finance;
- food;
- government;
- health;
- transport; and
- water.

203. Other countries and organisations may use a different list according to national priorities, but they are likely to be similar. It should be noted sectors are not listed in order of priority, as this depends on circumstances.

204. Not everything within a national infrastructure sector will be critical. But, within each sector there will be certain critical elements the loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services. In extreme cases, this can lead to severe economic or social consequences, or loss of life. These critical elements together make up the overall critical national infrastructure. They may be physical (sites, installations, equipment) or logical (information networks, systems). The key questions are:

- what role does space play in each of these?
- how is the availability or integrity of essential services reduced if the space segment is removed?

Assessing critical national infrastructure vulnerability

205. Once a critical national infrastructure and associated critical elements have been defined, we should conduct an assessment to determine specific vulnerabilities and address the:

- time-to-failure if a space capability is removed;
- effectiveness of backup services (if they exist); and
- underlying importance of space to the activity.

Understanding the relative importance of the activities allows finite resources to be targeted at the most critical areas of dependency, and also helps to create a business continuity model at a national level.

Phase 1 (Before) – Influencing actors in space

206. We have developed a six-step process to influence actors in space to encourage planners to get inside the actors' minds as shown in Figure 2.1 below. Steps 1-3 get planners to consider what drove an actor to select a harmful course of action. In steps 4-6, planners:

- consider whether it would be feasible to change the decision-making logic of the actor;
- identify mutually desirable end-states; and
- address essential elements of a plan to influence an actor in space.

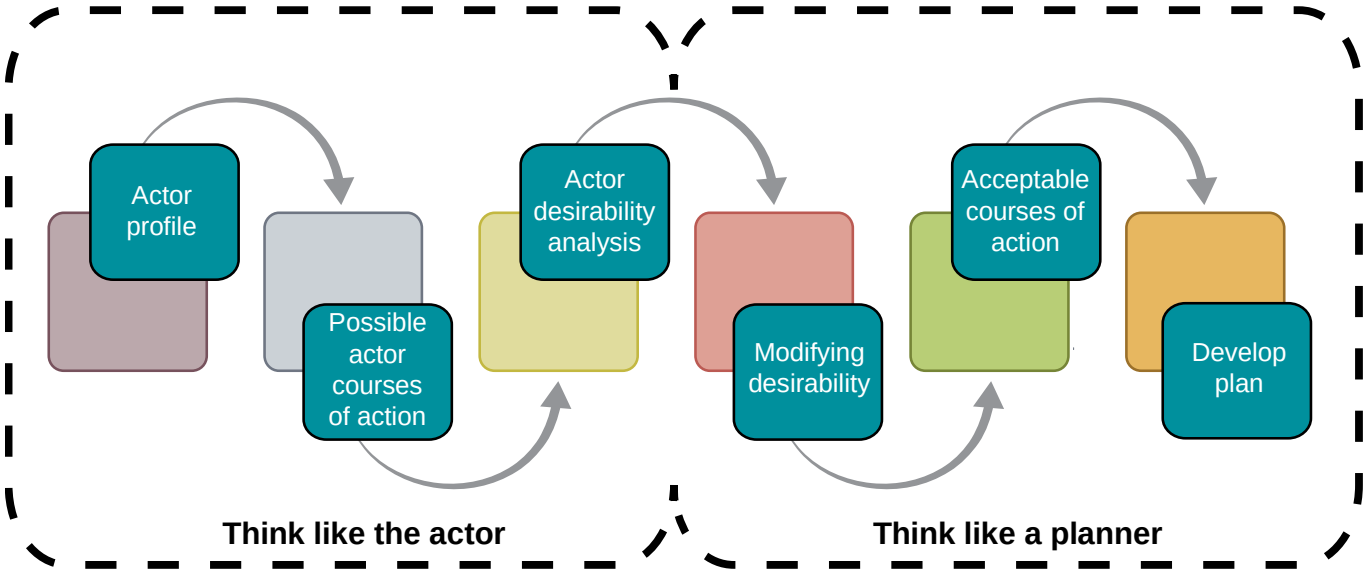

Figure 2.1 – The six-step process to influence actors

207. A significant input to the process is identifying the:

- developing crisis situation;
- actor;
- objective or harmful course of action;
- reason for the actor's behaviour, their motivations; and
- mechanisms the actor is likely to use to achieve their objective.

208. The process starts once a potential threat has been identified and attributed. Correctly attributing activities in space is difficult, and the national capabilities required to do so, are often highly classified. Deciding whether or not to reveal that a classified capability exists to an actor (for the sake of attribution) must form part of this planning process.

209. The six-step process is primarily concerned with addressing emerging crises and our reaction is one of '**immediate deterrence**'. This is where a crisis situation is just short of an attack, and it forces us to consider, or take, counter-measures. However, in any emerging crisis situation, there would have been some previous relationship between the parties in which a longer-term regulation existed. These regulated longer-term relationships are known as **general deterrence**. Focussing on immediate deterrence does not mean, however, that we have to wait for an actor to develop a capability to threaten space before we act.

Steps 1-3 – Thinking like the actor

210. In **Step 1: Actor's profile,** we need to reconstruct the actors' decision-making process to understand what made them choose a certain course of action and what the motivating factors were. Planners should consider the harmful course of action as, possibly, a symptom of a more fundamental root cause. They should also recognise that actors tend to act when they believe they have little choice, and often do so after considering the costs of not acting. A more detailed description of how actors arrive at decisions and how we can create their profile can be found at Annex 2A.

211. **Step 2: Possible course of action**. Actors use harmful courses of action to increase their safety, security, self-esteem, potential or, to avoid losses. Planners develop a list of possible courses of action available to the actor at the time they made a decision. It is possible that planners will identify additional courses of action of which the actor was unaware.

212. In **Step 3: Actor desirability analysis,** planners assess and rank courses of action by their desirability from the actor's perspective. Understanding actors' decision making is likely to require framing the selected course of action as a way of avoiding (or at least minimising) the perceived loss.

Steps 4-6 – Thinking like a planner

213. In **Step 4: Modifying desirability,** planners initially assess the size of the shift needed to replace the harmful course of action as the actor's most desirable choice. Planners consider how they may influence the actor's perception of the desirability of the harmful course of action by denying the benefits or increasing the costs. This could be achieved through '**deterrence by denial**' which aims to reduce the benefit of the actor's chosen course of action. Planners must then consider how to increase the benefits and reduce the costs of the alternative courses of action from an actor's perspective.

214. In **Step 5: Finding acceptable courses of action,** planners look for an attractive course of action for the actor that is acceptable to us. There is a tendency to focus on lawful counter-measures, but planners should also consider incentives that could increase the desirability of all acceptable alternative courses of action.

a. **Avoid 'tit-for-tat' strategies**. Given the vulnerability of space and our dependency on it, planners need to be cautious about adopting reciprocal (tit-for-tat) strategies. We should try to protect our access to space without causing any additional harm to the environment. For example, we may wish to influence an actor to consider terrestrial alternatives.

b. **Politically acceptable**. Our plan should consider leaving the actor with a 'face-saving exit' option, politically as well as militarily. If not, it could lead to undermining the actor's position domestically which may result in acts of self-preservation.

c. **Leverage**. Leverage should not be limited to physical targeting since the actor may not be susceptible to physical pressure points that can be destroyed. We should consider what the actor values and whether leverage against theses areas is likely to be effective.

d. **Cost**. Having identified a number of ways of modifying actors' courses of action, planners should work out the cost and whether we are willing to pay for it. This is not solely a monetary decision.

Other costs could be associated with relationships with allies or partners, prestige, or loss of diplomatic leverage.

215. **Balance of interests**. Analysing the relationship between the perceived interests of the involved parties is critical to understanding why an actor is not motivated to comply with our demands. Calculating the amount of force required to encourage a change in an actor's behaviour requires both a comparison of the parties' interests and intentions, as well as an assessment of their military capabilities. It is, in effect, a balance of interests. It has been claimed this balance of interests is a more important predictor of a crisis outcome than the balance of military power. Despite the threat of defeat or annihilation, weaker actors have not always been deterred by stronger actors due to an asymmetry of interests. Therefore, when the stakes are very high, some strategies may not succeed because a small chance of eventually prevailing is likely to motivate a weak actor to resist when they are unable to identify any viable alternatives – even if this requires paying a high price.

216. **Step 6: Developing the plan** is the final step of the process, planners identify factors that will affect four key components of a plan which, when combined, contribute to success. These are **clarity, communication, capability** and **credibility**. These considerations must be incorporated into existing crisis management activities and used to develop the plan.

Phase 2 (During) – Space defence

217. The protecting access to space study started with three major efforts: dependencies, vulnerabilities, and threats; deterrence; and collaborative mitigation. In considering protecting access to space we need to discuss space defence. This is a well-established discipline within spacefaring nations, although there is no commonly agreed doctrinal definition. The Joint Air Power Competence Center (JAPCC) produced a food for thought paper on *The Resilience of Spacecraft* which contains information on space defence.

218. Rather than proposing a comprehensive space-defence concept, this section focuses on space-defensive measures at the final stage of an attack on a spacecraft. These are best implemented through capability development *before* spacecraft are launched, including trade-offs between payload and protection. Space-defensive measures implemented *after* launch are likely to have a negative impact on spacecraft performance.

Space-defensive measures

219. Once in orbit a spacecraft is quite vulnerable. Its survivability is improved primarily through manoeuvring to avoid hazards or threats, and increasing its protection against radiation and debris. Electronic surveillance measures and electronic counter measures may also be used. Table 2.1 gives examples of some space-defensive measures.

Hazards and threats	Space defensive measure	Option(s)	System impact
Space weather	Increased protection	Radiation hardening	Increased cost, reduced payload
	Avoidance	Suspend operation	Reduced performance
Debris	Increased protection	Physical shielding	Increased cost, reduced payload
	Avoidance	Manoeuvre	Reduced performance, reduced lifetime
		Suspend operation	Reduced performance

Hazards and threats	Space defensive measure	Option(s)	System impact
Frequency fratricide – unintentional	Avoidance	Deconfliction	Reduced performance
		Suspend operation	Reduced perfomance
Direct attack (kinetic)	Avoidance	Manoeuvre	Reduced performance, reduced lifetime
	Increased protection	Physical shielding	Increased cost, reduced payload
Direct attack (cyber)	Avoidance	Suspend operation	Reduced perfomance
	Increased protection	Autonomous operation	Increased cost, reduced payload
		Encryption	Increased cost, reduced payload
Electronic attack	Avoidance	Suspend operation	Reduced perfomance
	Increased protection	Autonomous operation	Increased cost, reduced payload
		Encryption	Increased cost
Laser blinding	Avoidance	Suspend operation	Reduced performance
		Manoeuvre	Reduced performance
	Increased protection	Shutter/filter	Increased cost, reduced payload
Electro-magnetic pulse attack	Increased protection	Radiation hardening	Increased cost
	Avoidance	Manoeuvre	Reduced performance
		Suspend operation	Reduced performance

Table 2.1 – Examples of space-defensive measures

220. **Increased protection**. Designers use risk and vulnerability analysis simulation software to identify vulnerable components of a spacecraft. This allows them to harden, or shield, weak parts of the system. **Radiation hardening** will increase resilience against space weather and electromagnetic pulse attack, although it will not assure complete protection. Similarly, **physical shielding** offers a certain level of protection against kinetic attack and collision with debris. Both hardening and shielding adds

cost to the design, engineering, production and operation of the spacecraft. They also have an impact on spacecraft mass, thermal system complexity, power budget and material selection. Deciding to harden a spacecraft has an immediate impact on the payload. Each kilogramme dedicated to hardening the satellite is a kilogramme not available for the actual payload. Therefore, there is a dilemma between maximising the weight allocated to the payload to make the spacecraft as capable as possible, while protecting it against hazards and threats.

221. **Avoidance**. Risk and vulnerability analysis can also be used to reduce the spacecraft's working surface facing a hazard or threat. For example, the space shuttle flew backwards while in orbit to protect windshields against debris and micro-meteoroid impact. However, manoeuvring to avoid colliding may move a spacecraft into a sub-optimal orbit. This impacts on the payload performance and spacecraft lifetime. Manoeuvring is a complex process. It needs space situational awareness and careful consideration, from the capability development phase through mission planning and execution to make sure any manoeuvre is successful.

222. **Implications**. Space-defensive measures will have an impact on spacecraft operational effectiveness. Senior leaders need to be aware that taking early decisions in the design of a spacecraft will shape its survivability and such decisions become irreversible once the spacecraft is in orbit. Finally, it should be emphasised that the success of any space-defensive measure depends on continually monitoring the spacecraft, and its environment, to identify and analyse hazards and threats.

Phase 3 (After) – Collaborative space mitigation

223. While defence and deterrence contribute cooperatively to protecting space, it is possible that both measures may fail. A vulnerability gap exists between a growing dependence on space capabilities without a corresponding growth in spacecraft survivability. The absence of a mitigation strategy further widens this gap. The **collaborative space mitigation concept** provides nations with a strategy to manage the risk of disruption or denial effects on space capabilities due to the potential loss or degradation of space assets to hazards and threats.

224. A space mitigation strategy manages the risk of space defence and deterrence failing. It considers the probability and impact of a failure and provides a plan of action to keep the potential consequences at an acceptable level in a cost-effective manner. Space mitigation measures include those directed at the ground, communications and space segments to minimise the potential impact of hazards and threats on space capabilities.

Key elements

225. Collaborative space mitigation relies on partnership agreements and interoperability to propose a mitigation-strategy framework. This aims to exploit unused capacity to increase space capability resilience in a cost-effective manner. National approaches to space capability development may have served nations well, but are sub-optimal in delivering space capability within a multinational context.

226. Managing risk tends to keep our exposure to it to an acceptable level. If a spacecraft is degraded or lost, one method of limiting the impact would be to access alternative capabilities. For example, to manage the risk of losing a synthetic aperture radar satellite (used for wide-area surveillance over a nation's maritime approaches), one nation may elect to contribute its one synthetic aperture radar satellite to another nation's constellation. The resulting partnership not only provides both nations with access to information from the entire constellation, but also if one was lost, then contributing nations would still have access to the other nations' satellites.

227. Partnership agreements between nations and implementing interoperability standards and doctrine are two conditions for the effective and timely exploitation of unused space capacity. The concept manages the vulnerability gap by providing space capability developers with a mitigation strategy. This exploits unused space capacity through a combination of partnership agreements and interoperability protocols.

Options

228. We identified four space mitigation measures, namely:

- reverting to alternative (non-space) capabilities;
- replacement and redundancy of space assets;
- making alternative service arrangements; and
- collective responses.

229. **Reverting to some alternative capability** manages the risk of space disruption or denial with a plan to revert. This measure implies that the capability meets the requirements for capacity and timeliness. Nations that are dependent on space consider this mitigation measure to be of less value. This is because of the inadequacy for non-space capabilities to deliver true 'space-like' effects. This is particularly evident for reachback communication capabilities in support of deployed operations, deep-look intelligence, surveillance, and reconnaissance requirements in contested areas, and supporting precision-guided munitions.

230. **Replacement or redundancy of spacecraft** as a space-mitigation measure is costly in terms of both resources and the time required to replace spacecraft in orbit. So, this option is largely unattractive, particularly to commercial operators.

231. **Making alternate service arrangements** is a less costly space-mitigation measure. In the event of degradation or loss of a spacecraft, arrangements can be made with commercial vendors, but performance and responsiveness are likely to be less than that of the original system.

232. **Collective response** calls for separate space capabilities to act together to compensate for the loss or degradation of individual spacecraft. This depends on the willingness of the owners of such separate space capabilities to share with others. Thus developing a partnership agreement and implementing interoperability standards and protocols for sharing remains the challenge.

233. Table 2.2 summarises possible space mitigation measures and their impact.

Space mitigation options	Impact
Reverting to non-space capability	Requires excess, or surge, non-space capabilities May not provide the necessary requirements
Replacement and redundancy of space assets	Maintains performance and responsiveness Costly
Making alternate service arrangements	Affordable May lack performance or responsiveness
Collective response	Affordable with acceptable performance responsiveness Depends on the willingness to share space assets

Table 2.2 – Space mitigation measures

Five-step mitigation process

234. Developing a space mitigation strategy is a five-step process.

Step 1 – Identify the mitigation requirements[1]

Step 2 – Identify space capability functionality and redundancy

Step 3 – Identify partnership opportunities

Step 4 – Develop a space system integration framework to enable potential partnerships[2]

Step 5 – Implement the space system framework through operational, technical and architectural interoperability

[1] The requirement includes identifying payload capacity and capability, readiness and duration of service.
[2] For example, the Doctrine, Organisation, Training, Leadership, Personnel, Facilities and Interoperability framework could be used to do this.

An example showing how to apply the five-step process is shown below.

Using the five-step mitigation process

Using the Intelligence, surveillance and reconnaissance contributions to military and civilian maritime operations case study in MNE 7, *Space: Dependencies, Vulnerabilities and Threats,* we can show this process.

Step 1 – Mitigation requirements. The mitigation measure required may provide 50% of the original capability and make 25% of the capacity available within 48 hours of space asset loss for a minimum of six months.

Step 2 – Space capability functionality and redundancy. Here, we identified the latent space capability available to address our mitigation requirements. Surveillance and data collection, as expressed in the *Space: Dependencies, Vulnerabilities and Threats* case study, are the functionalities needed.

Step 3 – Partnership opportunities. We could get surveillance through an information and data exchange agreement with another nation. Data collection could be achieved through arrangements with commercial or government providers of synthetic aperture radar capabilities. This is where political acceptability of the partnership agreements will be assessed.

Step 4 – System integration framework. Assuming an agreement is in place, we need to develop procedures to assure data exchange. This will include developing data-transfer protocols, and tools and hardware to enable the physical transfer of data. We must realise the cost implication of such a mitigation strategy. In this example, we may need to construct a ground station and provide engineering support to receive data in the agreed format.

Step 5 – Implementing interoperability. Once a framework has been developed at Step 4, we need to implement it through a process of *operational*, *technical*, and *architectural* interoperability. For example, the Canadian Reconnaissance Operational Workstation Exploitation (CROWE) prototype was developed to receive commercial imagery and insert it into strategic, operational and tactical commanders' information environment in near real-time. To achieve its mission, CROWE needed interoperability with a network to the three levels of commands, such that CROWE could access the request for information, retrieve the commercial imagery, adapt the size and format of the space product, and then disseminate.

Annex 2A – How actors make decisions

2A1. Within the context of this framework, ‘rational’ has a particular meaning. We assume that rational decision-makers will rank possible courses of action by their desirability. The rational decision-maker acts on those preferences, choosing the one with the highest desirability from a list of possible courses of action. Within the theory, there is an understanding that information may be incomplete and not all possible courses of action considered. This may result in bad decisions. But, decision-makers are rational if they choose the most desirable option from their perspective.

2A2. Incorporating factors outside of the rational decision-maker model will help planners to determine an actor’s decision-making process more accurately. This should result in more effective planning. The model is useful. However, failures to deter actors from courses of action indicate that some assumptions and simplifications made do not fit reality. Generally, rather than taking risks to maximise gains or benefits, many actors take significant risks to minimise losses. Under certain conditions some disregard cost-benefit calculations altogether. The organisational structure in which the decision is made can frequently amplify, frustrate, or even pervert the intentions of decision makers.

Modifying the rational decision-maker model

2A3. Using the rational decision-makers idea is widely acknowledged because it is simple and logical. We should also include other factors.

a. **Endowment effect**. There is a tendency for planners to underestimate the benefit of ownership or the cost an actor will find acceptable in order to give up something they perceived as theirs.

b. **Problem framing**. Problem framing means that identical problems can result in different choices if presented in another way.

c. **Present-bias**. Actors will show a preference for a reward that arrives sooner rather than later. Consequently, actors discount courses of action that deliver benefits in the longer-term.

d. **Prospect theory**. Rather than being risk-seeking or risk-adverse, actors facing deteriorating situations tend to be more willing to take risky actions, when the model might predict a preference for restraint.

e. **Omni-balancing**. When considering an actor's decision making, it is a common mistake to underestimate the value attached to personal security in relation to threats originating internally, as opposed to external threats.

f. **Rubicon theory**. The Rubicon theory explains a difference between decision-making processes before, and after, a course of action has been selected. It is important to influence the actor early enough in the process. Otherwise the perceived costs of demands will be discounted if a decision has been made.

g. **Dominant behaviour**. There is evidence that some actors tend to engage in displays of dominant behaviour. In plain language, some actors, under specific conditions, like to fight. These actors are less likely to act in accordance with the rational decision-maker model.

h. **Organisational model**. The organisational model suggests that momentum exists behind organisational decisions. This makes changing a decision or course of action more difficult. Also, an organisational structure can obscure the way in which a decision was made, making it more difficult to influence or deter.

i. **Politics model**. The politics model reasons that government decisions are a result of politics, bargaining, idea sharing and power playing. Therefore, we need to identify the games and players involved.

Conclusions

1. Space is everybody's business. Almost all nations – spacefaring or not – depend on space. Given the wide availability of space capabilities across every aspect of daily life, the responsibility for protecting access goes beyond the narrow cadre of space professionals. The vulnerability of the space environment to hazards and threats requires a much more proactive and collaborative approach to implementing a comprehensive range of measures. As well as being prepared to deal with the consequences of disruption and denial of space, we must anticipate and manage risks before they arise.

2. **Identifying dependencies**. Since all nations depend on space to some degree, they need to identify and prioritise specific dependencies and vulnerabilities. This can be accomplished using the UK's national critical dependencies concept. It will create a business continuity model to address the loss of space capabilities at a national level. However, this represents only the first step. Protecting access to space requires identifying communities of shared interest as a basis for multinational collaboration.

3. **Deterring and influencing in space**. Preventing actions materialising that threaten space capabilities, is better than dealing with their consequences. Therefore, proactive engagement through deterrence and influence is essential. To be successful, it will be important to identify an outcome that is acceptable to all parties. This publication provides a process to guide decision-makers and planners and should be integrated into strategic planning and crisis management procedures.

4. **Collaborative space mitigation**. Unused space capacity exists and represents an opportunity to improve access to space. However, while potentially cost-effective, this approach will depend on a willingness to collaborate as well as political acceptability and interoperability. The collaborative space mitigation concept offers a framework to develop affordable and sustainable partnerships that keep the potential impacts of disruption or denial of space at acceptable levels.

5. **Space defence**. Protecting access to space means we need to defend our space assets. This is a well-established discipline within spacefaring nations, although there is no common doctrine. So, rather than proposing a comprehensive space defence concept, we discussed some of the more common space-defensive measures available to protect spacecraft from hazards and threats. Such measures are best incorporated through capability development before launching them into space because if implemented afterwards, they will have a negative impact on performance.

6. **Space situational awareness**. We have developed this framework assuming there is a sufficient level of space situational awareness. This capability is vital to successfully deter and influence, defend and mitigate disruption or denial of space.

Way ahead

7. We have proposed a framework for protecting access to space. Nations are free to implement any or all of the processes outlined. However, the current approach is unsustainable and is putting access to space – and the capabilities it delivers – at risk. This has significant consequences for our economic, societal and national security.

8. Raising awareness of our dependency on space is fundamental. This requires an ongoing process of education. This guide, and its supporting products, provides a body of material that nations or organisations can use.

9. Maturing the concepts for deterring and influencing actors in space, and collaborative mitigation will require further concerted, multinational effort. Given the terms of reference of this campaign, further work is necessary to deepen our understanding of the specific application of these concepts. In particular, analysis to establish the effectiveness of the proposed framework will increase confidence in the model. Also, the potential to apply the conceptual framework in other domains – specifically cyber – should be pursued.

Annex A – MNE 7 outcome 2 products

Space: dependencies, vulnerabilities and threats handbook

A1. *Space: dependencies, vulnerabilities and threats* handbook is aimed at audiences working in a range of military and civilian specialist and generalist areas. We tried to create a main body of text which acts as a basic space primer, so that users can develop a simple, but sufficient, understanding of the key capabilities that space-based systems could provide. An important element of this is an understanding of:

- different orbits that are available;
- what space-based systems can do; and
- generic vulnerabilities of, and threats to, space-based systems.

A2. The handbook includes ten case studies on the use of space, ranging from agriculture to time-sensitive targeting. These aim to take all of the information presented in the handbook to show how space capabilities are used.

A process to influence actors in space

A3. Actors in space must be motivated to pursue courses of action that do not disrupt or threaten our access to space. Overall the aim of the product is to provide guidance on deterring and influencing to increase the likelihood that an actor will behave in an intended manner. This product identifies how to manage the behaviour of actors who threaten access or use of space. It is designed such that it could be integrated with political-strategic crisis management processes.

A deterrence primer

A4. The deterrence primer identifies and collates key deterrence knowledge in one place. It includes a history of the development of the typology of deterrence and describes and defines important terms. Since deterrence concerns influencing the actions of an individual or a group, the primer outlines the major theories that describe decision-making as it relates to

deterrence. Specifically a principal theory of the rational actor model and supporting theories that modify the ideas outlined within it.

Collaborative space mitigation concept

A5. The collaborative space mitigation concept addresses proactively the risk of the disruption or denial of key space capabilities through collaboration. Using latent space capacity, partnerships, and interoperability the concept offers a potentially cost-efficient strategy for managing the risk of disruption or denial of space access. This product informs operational-level commanders and staff, national-level decision-makers, civilian bureaucrats, and industry, and could serve as the foundation for the development of national and international policies, strategies and capabilities.

Space mitigation survey

A6. A space mitigation survey was developed to review the defence community's perception of dependence on space assets and their knowledge of existing mitigation approaches in case of degradation or loss of access to the capabilities. The results of the survey showed that short disruptions are perceived to have moderate impact while long disruptions have extreme impacts on operations. Respondents' knowledge of mitigation measures was limited to returning to old technologies and procedures or using alternative means (for example, high-altitude airships).

A7. The results support the view that better mitigation approaches need to be developed. We should also implement training and exercises focusing on the employment of these approaches.

Protecting access to space

A8. The *protecting access to space* workstrand draws selectively on products from the objectives as well as a 'food for thought' paper on resilience provided by the Joint Air Power Competence Centre (JAPCC). Intended for use by spacefaring and non-spacefaring nations, this guide provides senior decision-makers with a strategic overview of dependencies on space and gives them options on how we can protect our access to it.