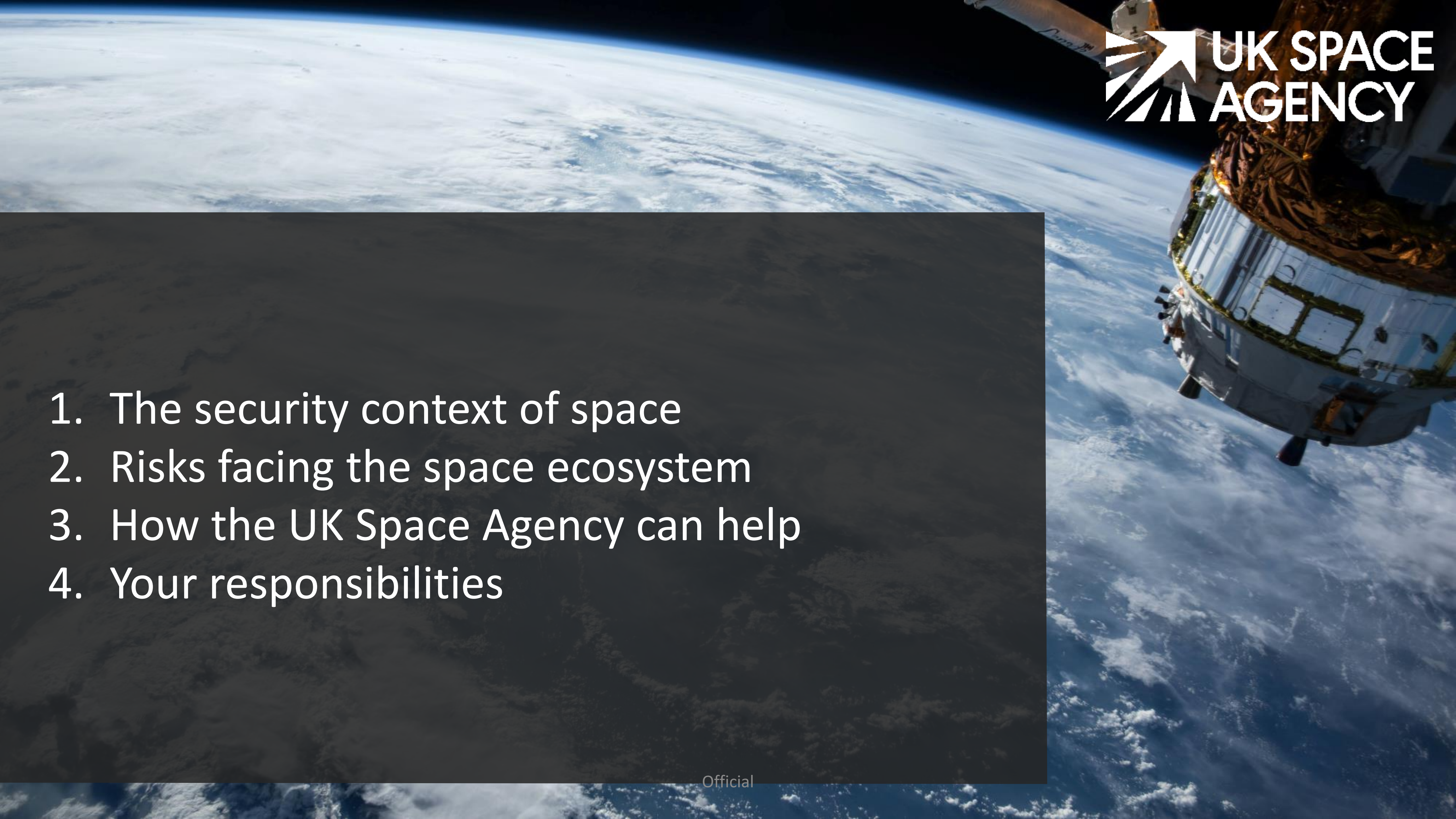
UK SPACE AGENCY

Developing Resilience in the Space Ecosystem: What hazards and threats you could encounter and how to prepare

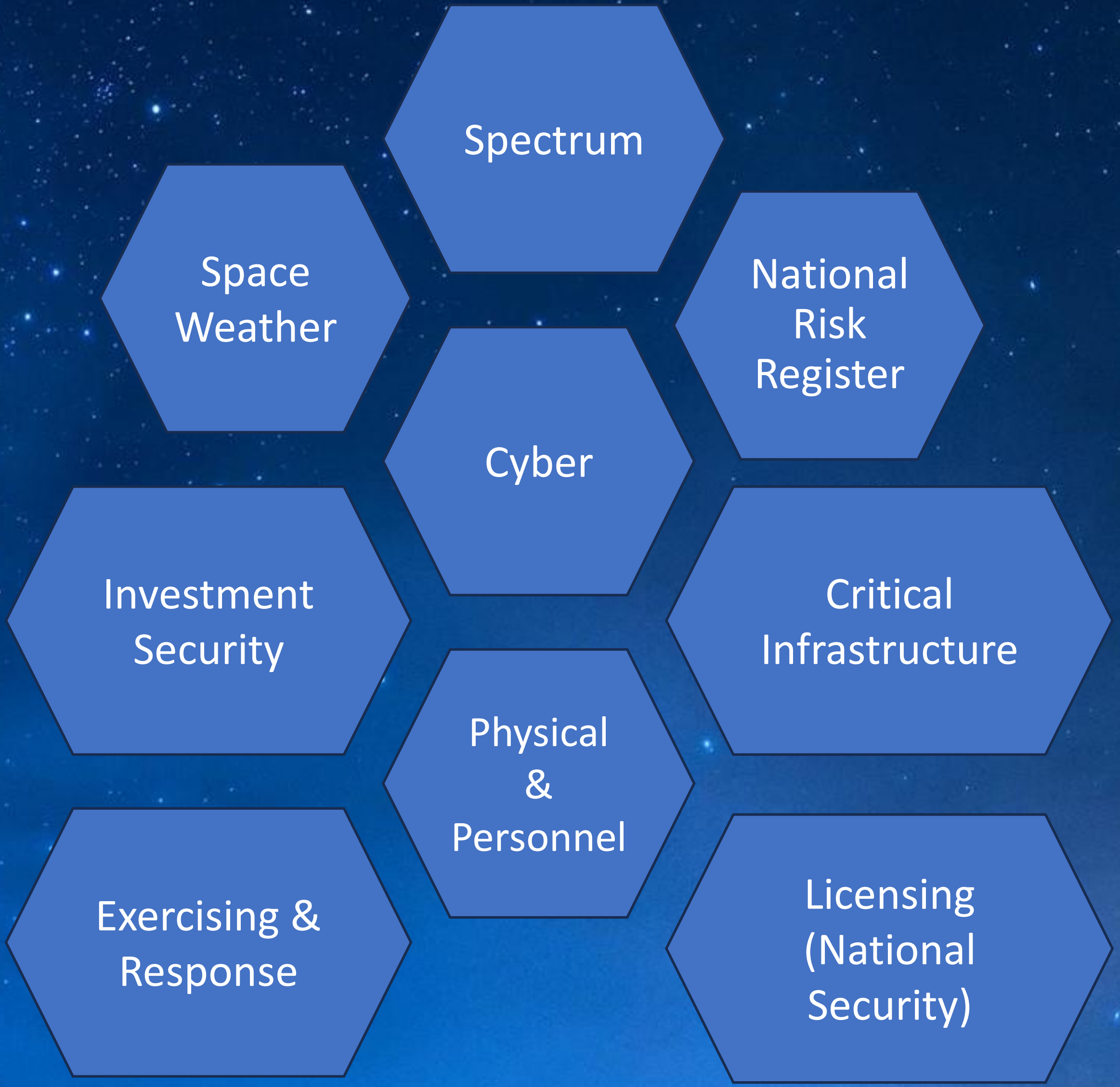
Official



1. The security context of space
2. Risks facing the space ecosystem
3. How the UK Space Agency can help
4. Your responsibilities

UKSA Security & Resilience

- UK Space Agency executive agency to Department of Science, Innovation and Technology
- Space operations, and security thereof involves a number of government players; MoD, FCDO, DfT, DSIT
- Small, but agile and wide ranging team covering policy areas:



Spectrum

Space Weather

National Risk Register

Cyber

Investment Security

Critical Infrastructure

Physical & Personnel

Exercising & Response

Licensing (National Security)

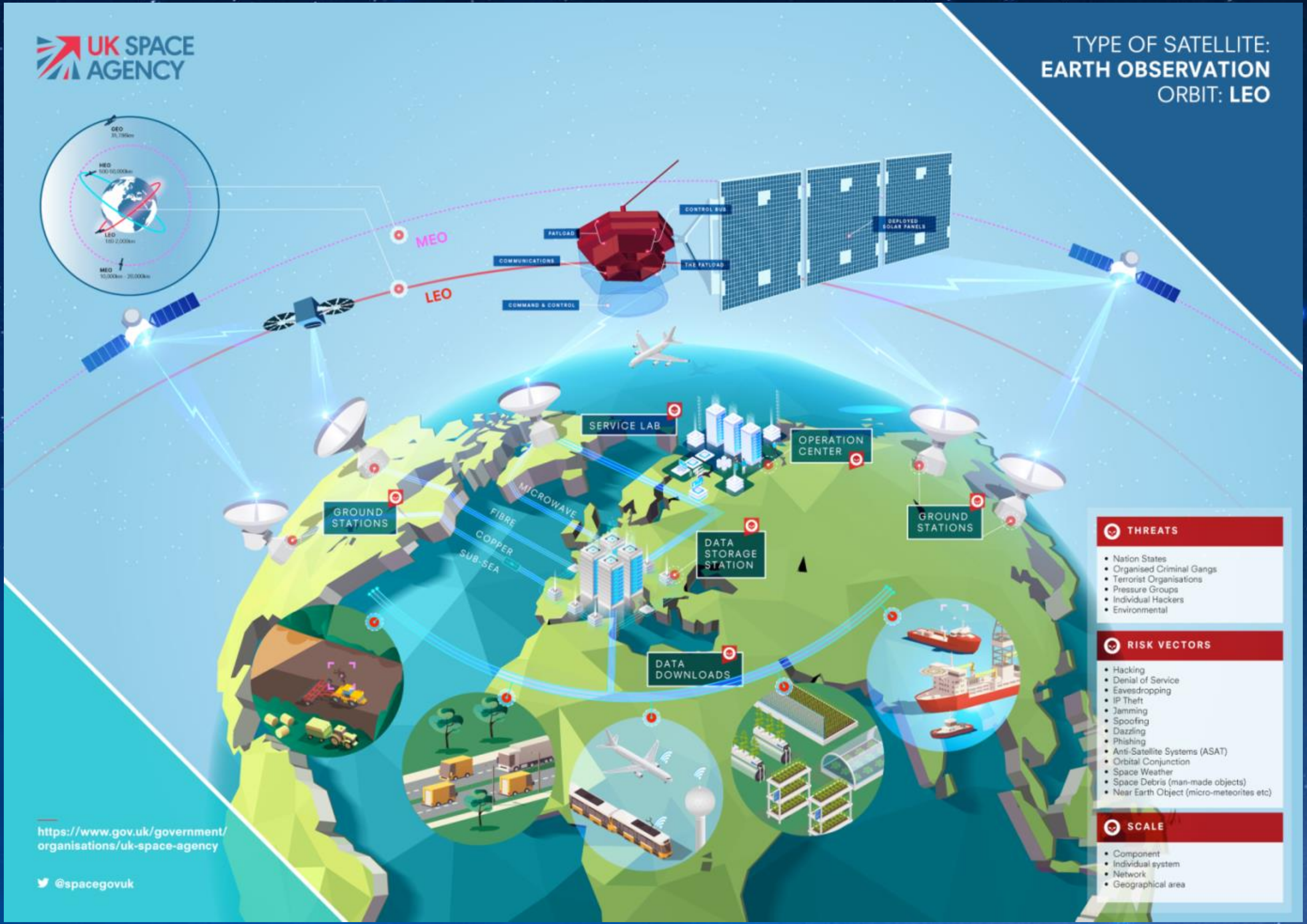
UK SPACE AGENCY

Security context of space

- Space provides capabilities and potential for economic and national security advantages
- Developed from just State Actors to include private interests
- Congested, contested and competitive
- Space economy valued by $1.8trillion by 2035 (*World Economic Forum)*
- Dual-use vs dual-purpose
- Outer Space Treaty* (1967)
- **The Treaty on Principles Governing the Activities of States in the Exploration Use of Outer Space, including the Moon and Other Celestial Bodies*

The Space Ecosystem

“communities of hierarchically independent yet interdependent heterogeneous participants who collectively generate an ecosystem value proposition.”



THREATS

- Nation States
- Organised Criminal Gangs
- Terrorist Organisations
- Pressure Groups
- Individual Hackers
- Environmental

RISK VECTORS

- Hacking
- Denial of Service
- Eavesdropping
- IP Theft
- Jamming
- Spoofing
- Dazzling
- Phishing
- Anti-Satellite Systems (ASAT)
- Orbital Conjunction
- Space Weather
- Space Debris (man-made objects)
- Near Earth Object (micro-meteorites etc)

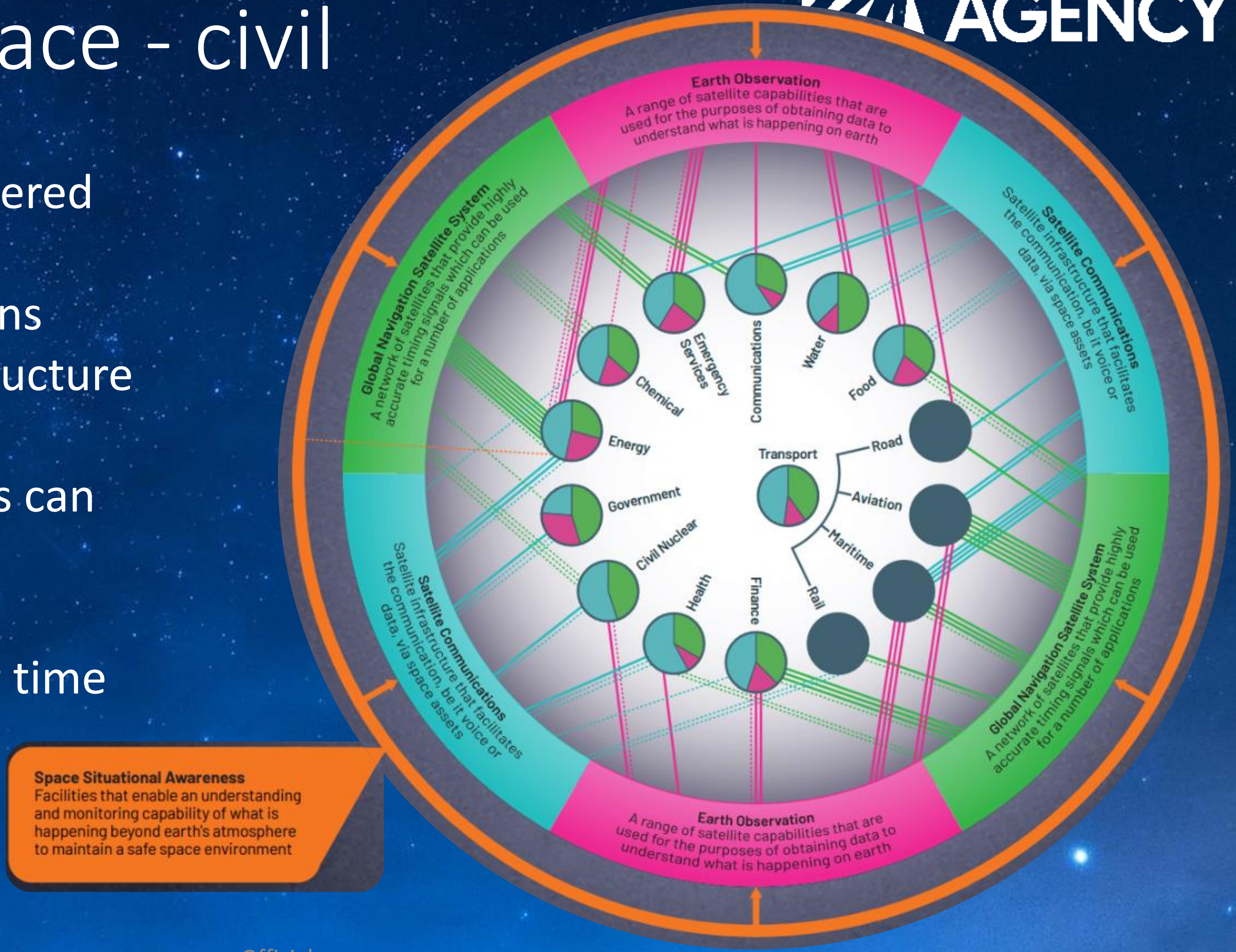
SCALE

- Component
- Individual system
- Network
- Geographical area

UK SPACE AGENCY

The utility of space - civil

- Space is increasingly considered civil infrastructure
- Supports a range of functions within other critical infrastructure sectors
- Disruption to space services can result in cascading impacts through other systems
- Dependencies emerge over time
- Supports 18% of UK GDP (~£370bn)



Earth Observation
A range of satellite capabilities that are used for the purposes of obtaining data to understand what is happening on earth

Satellite Communications
Satellite infrastructure that facilitates the communication, be it voice or data, via space assets

Global Navigation Satellite System
A network of satellites that provide highly accurate timing signals which can be used for a number of applications

Space Situational Awareness
Facilities that enable an understanding and monitoring capability of what is happening beyond earth's atmosphere to maintain a safe space environment

Securing Innovation

“The security threat to the UK emerging tech industry is growing. But many such businesses remain vulnerable to attack.”

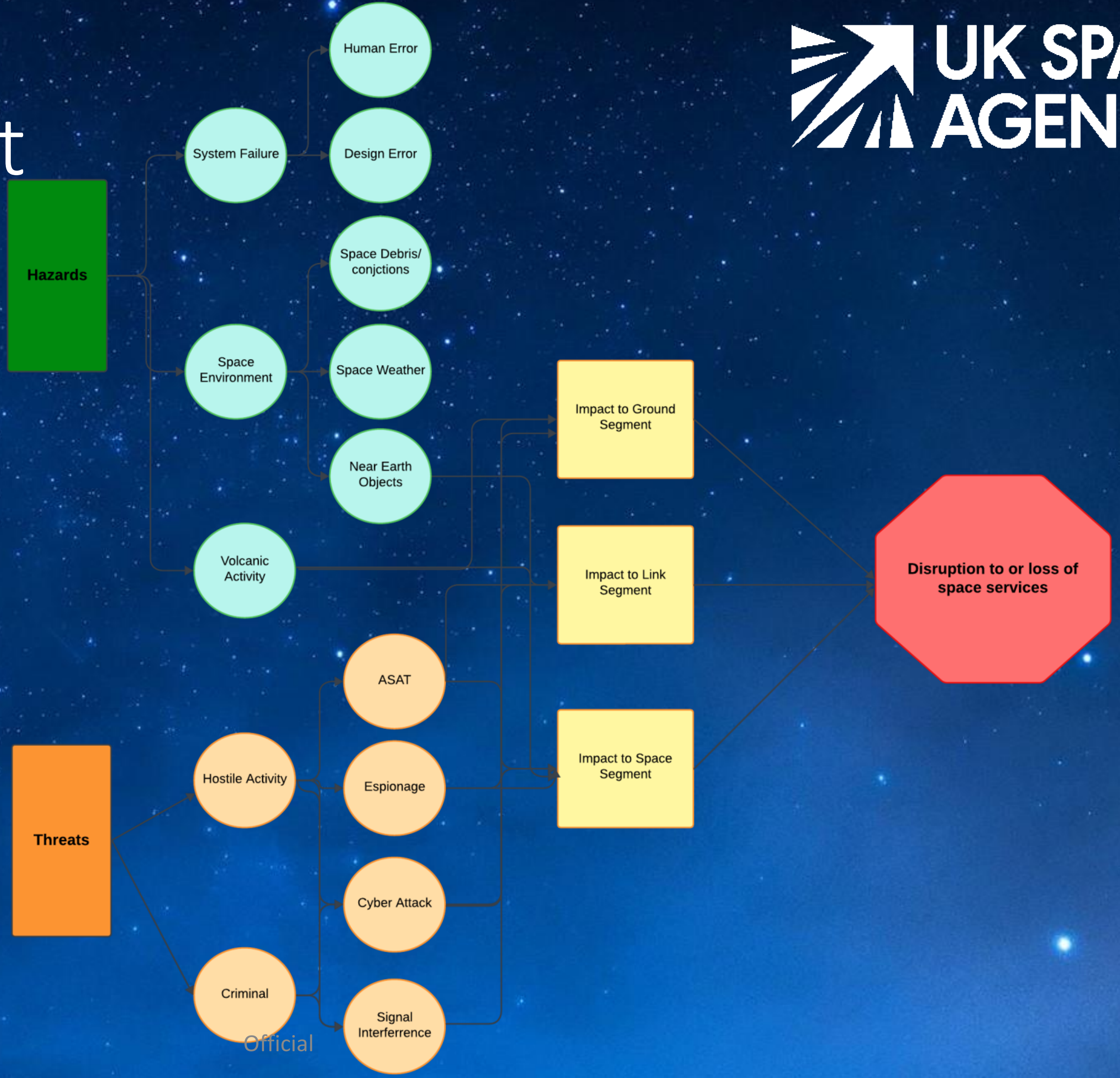
1. **Know Your Threats**
2. **Secure Your Environment**
3. **Secure Your Products**
4. **Secure Your Partnerships**
5. **Secure Your Growth**

Search ‘Secure Innovation NPSA’

SECURE INNOVATION

UK SPACE AGENCY

Security context



Hazards

System Failure

Human Error

Design Error

Space Environment

Space Debris/ conjctions

Space Weather

Near Earth Objects

Volcanic Activity

Threats

Hostile Activity

Criminal

ASAT

Espionage

Cyber Attack

Signal Interferrence

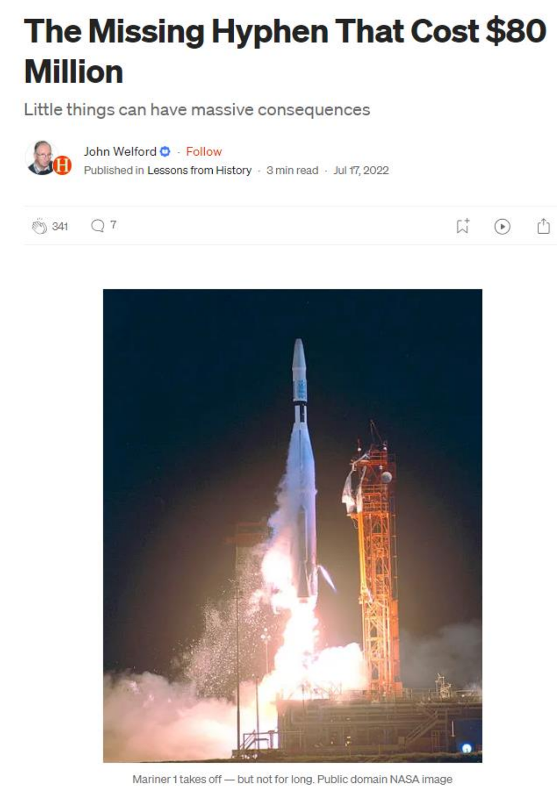
Impact to Ground Segment

Impact to Link Segment

Impact to Space Segment

Disruption to or loss of space services

Accidental/ Hazards



The Missing Hyphen That Cost $80 Million

Little things can have massive consequences

John Welford · Follow

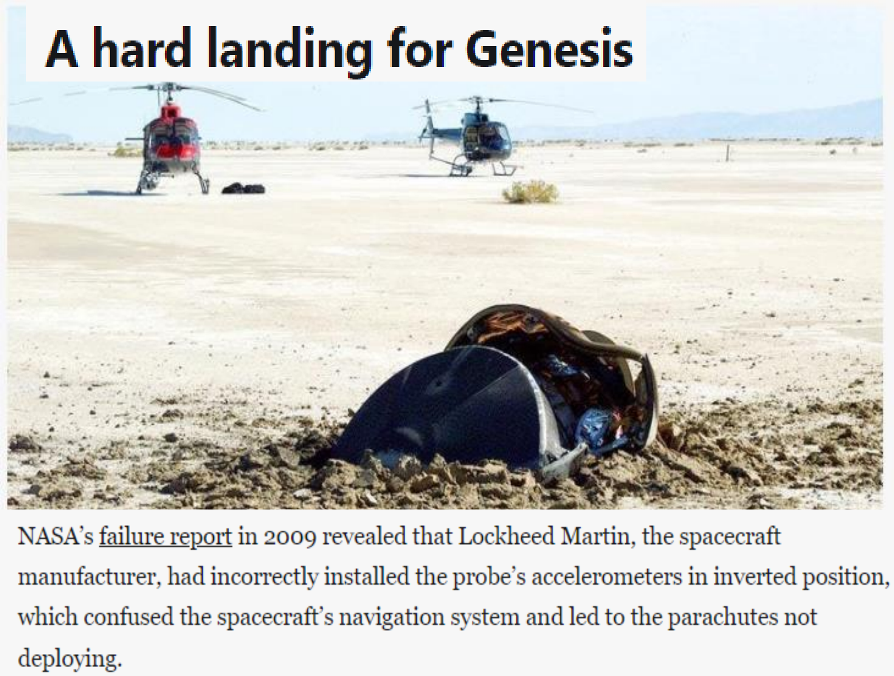
Published in Lessons from History · 3 min read · Jul 17, 2022

341 7

Mariner 1 takes off — but not for long. Public domain NASA image

SpaceX loses 40 satellites to geomagnetic storm a day after launch

9 February 2022

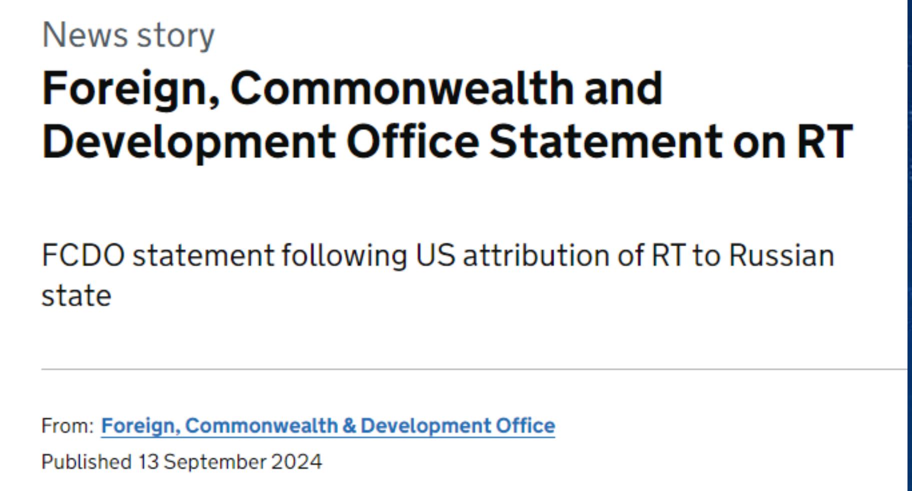


A hard landing for Genesis

NASA's failure report in 2009 revealed that Lockheed Martin, the spacecraft manufacturer, had incorrectly installed the probe's accelerometers in inverted position, which confused the spacecraft's navigation system and led to the parachutes not deploying.

UK SPACE AGENCY

Threats / Malicious



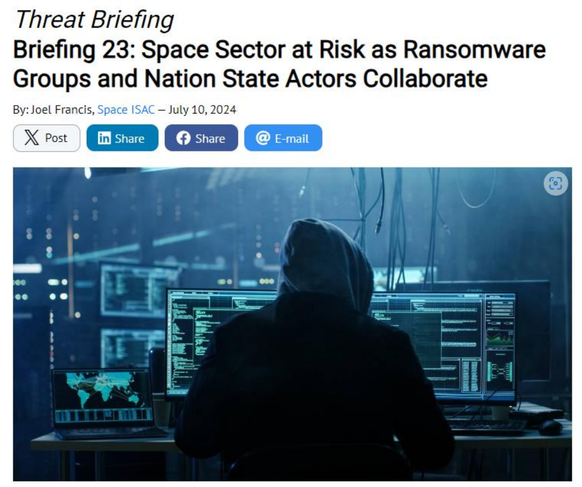
News story

Foreign, Commonwealth and Development Office Statement on RT

FCDO statement following US attribution of RT to Russian state

From: Foreign, Commonwealth & Development Office

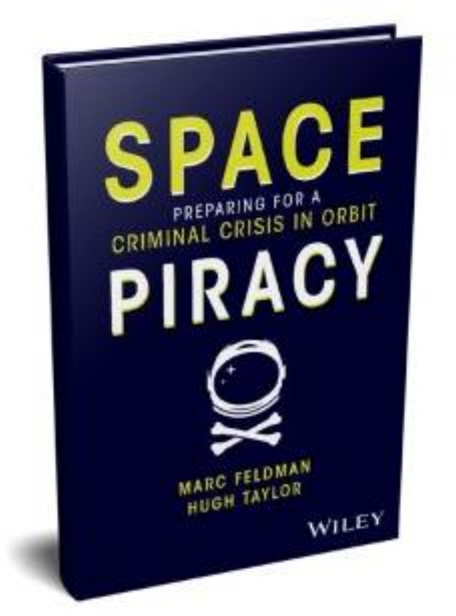
Published 13 September 2024

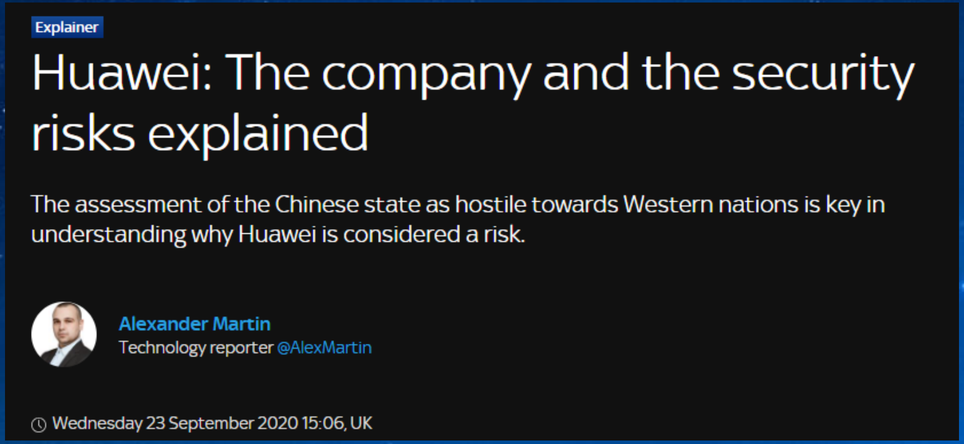


Threat Briefing

Briefing 23: Space Sector at Risk as Ransomware Groups and Nation State Actors Collaborate

By: Joel Francis, Space ISAC – July 10, 2024





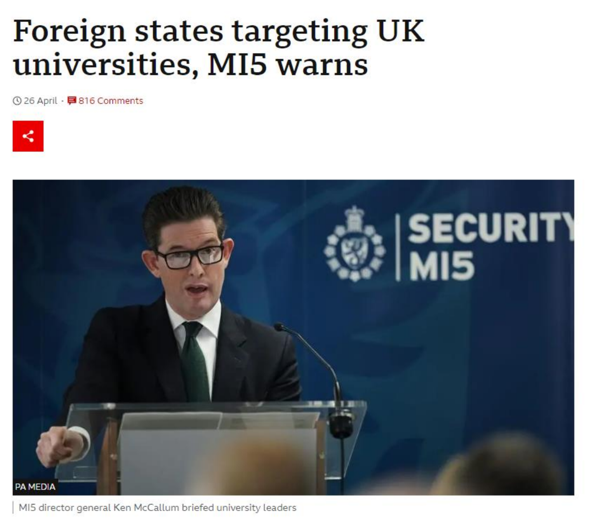
Explainer

Huawei: The company and the security risks explained

The assessment of the Chinese state as hostile towards Western nations is key in understanding why Huawei is considered a risk.

Alexander Martin
Technology reporter @AlexMartin

Wednesday 23 September 2020 15:06, UK



Foreign states targeting UK universities, MI5 warns

26 April · 816 Comments

MI5 director general Ken McCallum briefed university leaders

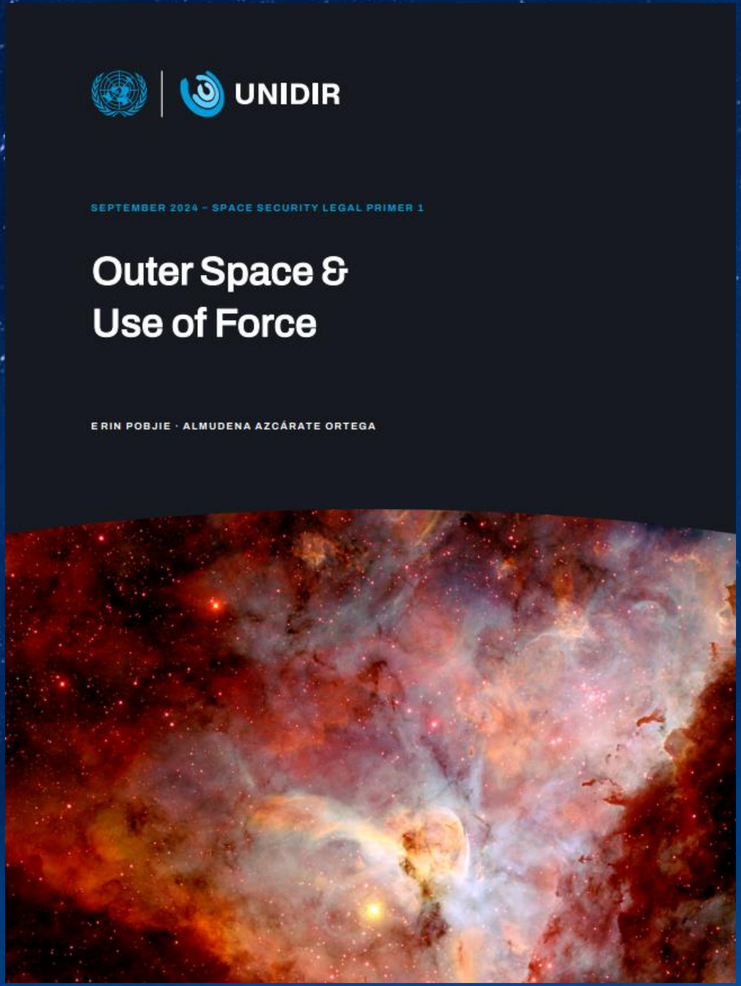
By Nathan Williams

Activism

STOP THE GENOCIDE
ISRAELI WEAPONS MADE HERE
#STOP ARMING
ELBIT SYSTEMS KILLS KIDS FOR CASH
MADE IN BRISTOL WEAPONS OF GENOCIDE

The people of Bristol just BLOCKADED Elbit over it's support for Israel's genocide

Use of force



UNIDIR

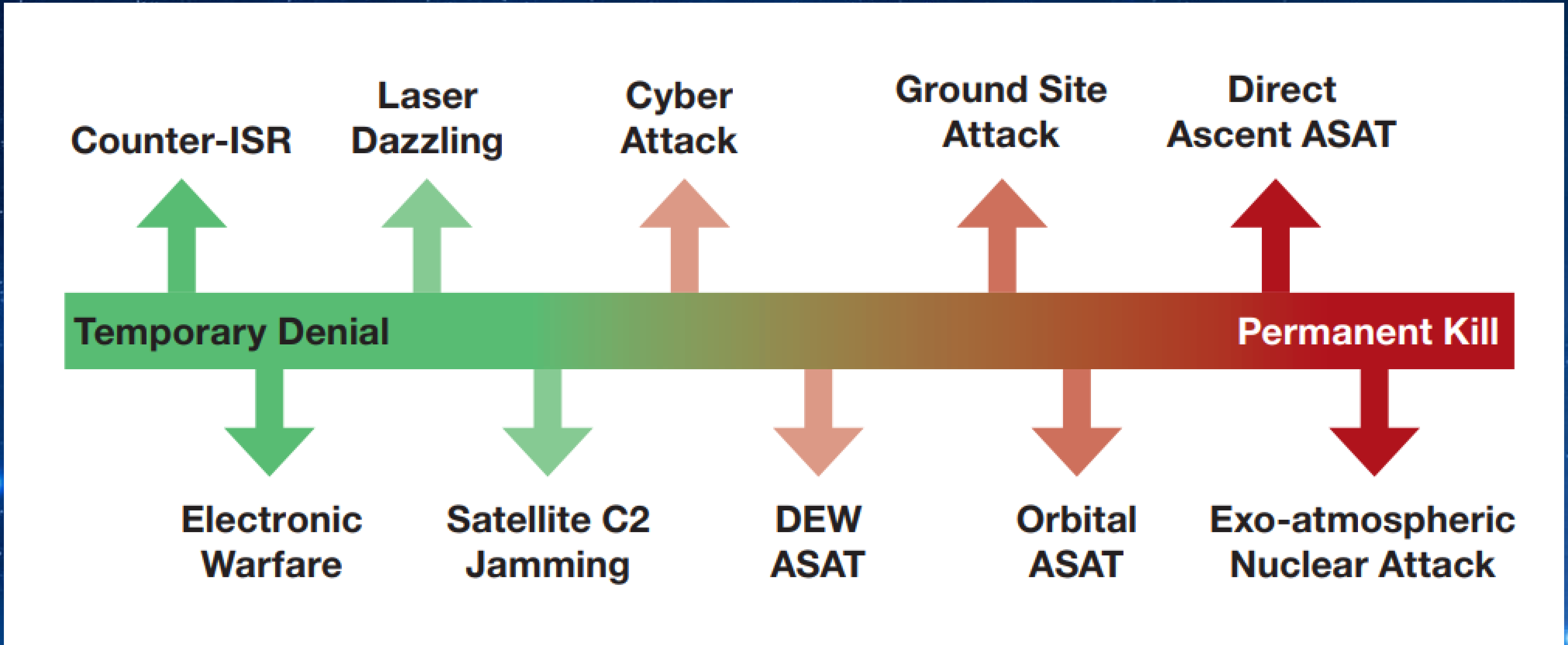
SEPTEMBER 2024 – SPACE SECURITY LEGAL PRIMER 1

Outer Space & Use of Force

ERIN POBJIE · ALMUDENA AZCÁRATE ORTEGA

- OST brings into force the UN Charter to Outer Space – prohibition of the use of force
- Use of force elements include: context, effects, gravity and intention
- Does not exclude certain capabilities and behaviours
- Lack of clarity in meaning of

Counter-space weapons



Help and support

Everyone needs to protect intellectual property, assets and services from malign actors and accidental events.

Demonstrating a commitment to security is critical to the ongoing success of any business. Ensuring secure, robust and recoverable services, systems and processes can provide a competitive advantage in the marketplace and avoid unnecessary costly retrofitting.

Cyber & Digital Security

Cyber Essentials

Cyber Essentials is an effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Self assessment vs technical verification (Plus)

Secure by Design

The foundations required for embedding cyber security practices in digital delivery and building resilient digital services.

1. Establish the context
2. Make compromise difficult
3. Make disruption difficult
4. Make compromise detection easier
5. Reduce the impact of compromise
6. Recovering from compromise

Secure by Design

1	**Establishing the context**	Understand your threats and vulnerabilities and determine all the systems which support the delivery of your critical functions.
2	**Making compromise difficult**	An attacker can only target the parts of a building and system they can reach. Make these as difficult to penetrate as possible
3	**Making disruption difficult**	Design systems that are resilient to attack and failure.
4	**Making compromise detection easier**	Design your systems so you can spot suspicious activity as it happens and take the necessary action quickly and effectively
5	**Reducing the impact of compromise**	If an attacker succeeds in gaining a foothold, they will then move to exploit your systems. Make this as difficult as possible by segmenting and separating systems.
6	**Recovering from compromise**	Develop systems than can be recovered from a major compromise; have effective and tested plans and procedures in place. Backup solutions and fallback procedures are vital to the ongoing successful running of your business

Breakout #1

How can you apply Secure by Design principles within your mission concept?

Cyber & Digital Security

Ground Station Technical Specification

UKSA initiative to developed a tiered specification which operators can voluntarily look to align themselves to.

Regulatory Review

- EO Data Security policy and wider space-data regulations
- Embedding national security and interest consideration in licensable space activities
- Creation of appropriate and proportionate requirements for protection of space systems

Partnerships

- WHY are you collaborating?
- WHO are you working with?
  - Background checks – see *NPSA Background Checks Guidance*
- WHAT are you sharing?
- HOW are you protecting your innovation?
  - Non-disclosure and other agreements

Personnel & Physical Security

Trusted Research

Advice and guidance published jointly by NPSA and the NCSC which supports the integrity of the system of international research collaboration. Designed in partnership with the sector, it provides guidance to researchers, university staff and funding organisations to help keep sensitive research and intellectual property secure from theft, misuse or exploitation.

Informed Investment

There are potential risks associated with investment - both to your business and the UK's national security - and how taking a security-minded approach from the start of your investment planning can reduce these risks.

National Protective Security Authority

Organisational

Business Continuity

Business continuity management (BCM) is a strategic framework that enables organizations to **rapidly restore their operations in the event of a disruption** or crisis. It involves identifying potential risks, such as natural hazards or cyberattacks, and implementing measures and protocols to reduce the impact of such adverse events on business operations. BCM ensures that critical business functions can continue or **quickly resume** during and after a disruption, thereby **minimizing financial and operational damage**.

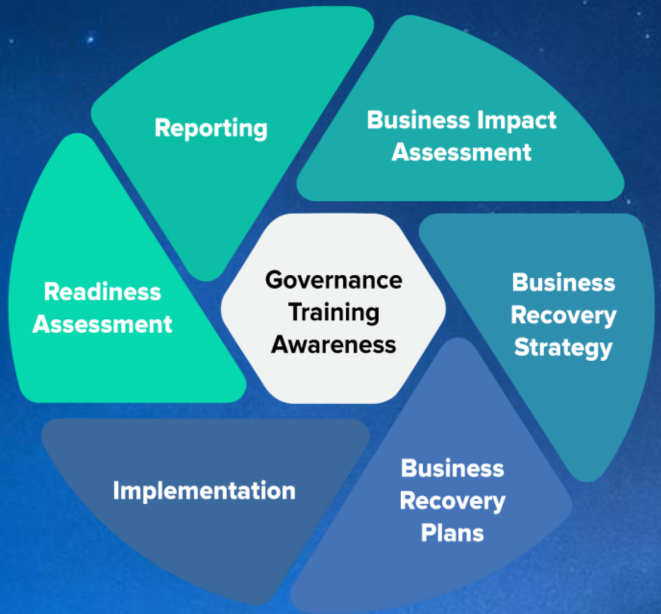
See resources:

Business Continuity Management Toolkit – gov.uk

Business Continuity Institute

ISO 22301 – Business Continuity Management Systems

'Off the shelf' books


Reporting
Business Impact Assessment
Readiness Assessment
Governance Training Awareness
Business Recovery Strategy
Implementation
Business Recovery Plans

In summary…

- You are part of the space ecosystem, network of relationships
- Dual-use brings about particular hazards and threats
- Secure your innovations
- Range of open programmes and guidance to help get you started