UNIVERSITY OF BATH

Citation for published version:
Blondel, P 2021, *Defence of space-based assets*.. <https://post.parliament.uk/research-briefings/post-pn-0654/>

Publication date:
2021

Document Version
Publisher's PDF, also known as Version of record

Link to publication

University of Bath

UK Parliament POST

POSTNOTE

Number 654 September 2021

Defence of space-based assets

Overview

- Space-based assets are critical national infrastructure, enabling many key services.
- Satellites are vulnerable to deliberate attack, space weather, and collisions with debris or other satellites.
- The numbers of satellites and satellite operators are growing, increasing levels of space debris and the chances of collisions.
- The US, Russia, China, and India have tested anti-satellite missiles in space.
- Mitigation strategies include removing debris from orbit, setting up terrestrial alternatives, and technical defences to hinder attack.
- The UK owns military satellites for communications but relies on allies for other defence-related satellite services.
- The UK plans to spend £6.4 bn on space defence capabilities over the next 10 years.

Space-based assets (satellites and the terrestrial ground stations that communicate with them) provide critical support to military and civilian operations. They are vulnerable to unintentional damage and disruption, and to deliberate attack. This note outlines how the UK uses and accesses satellites, potential risks to satellites, and approaches to mitigation.

Background

Space-based assets are considered part of UK critical national infrastructure,[1] and are important for civilian activities in many sectors, such as transport, finance and utilities.[2] They are also central to military operations, for example, for surveillance, communications, navigation and ballistic missile detection.[3,4] The UK space industry was estimated to support 45,100 jobs and to generate income of £16.4 bn per year, in 2018/19.[5] Satellite services also support the wider economy. In 2018/19, at least £361 bn of UK GDP was estimated to come from non-financial industries that were supported by satellite services.[6,5] Disruption to satellite services could have significant financial impacts.[7] In 2017, the London Economics consultancy estimated that a five-day disruption to global navigation satellites might cost the UK £5.2 bn.[8]

Space is becoming an increasingly congested, contested and complex environment.[9] Early space activities were dominated by the US and the former Soviet Union, however, technological developments and falling costs have allowed many other states and companies to develop space capabilities.[4,10–12] In the past decade, China, Russia and India have expanded their space programmes (including anti-satellite missile capabilities), and many other nations have set up their own space programmes. UK defence relies heavily on space-based assets, and evidence presented to the Commons Defence Select Committee suggests that this dependence is likely to increase in the future.[13]

Commercial activity is also increasing. The number of active satellites orbiting Earth has risen from approximately 2200 in Feb 2020, to almost 4100 in May 2021.[14,15] 73% of satellites provide services to commercial users, and this is set to rise.[14,16,17] In the next decade, firms such as SpaceX, Amazon and OneWeb aim to launch constellations of thousands of low-cost satellites into low-Earth orbit (160-2000km above the Earth) to provide global broadband services.[18–22]

In its Integrated Review of Security, Defence, Development and Foreign Policy, the UK Government set out its ambition to be able to monitor and defend UK interests in space by 2030 (Box 1). It said that in 2021 it will publish a defence space strategy (originally due in 2018) as well as a national space strategy.[23,24]

UK use of space-based assets

Satellites transmit information via radio signals. Ground stations send data (including operating instructions) to satellites, and satellites send data to ground stations, users or other satellites. Satellites usually provide one or more of the following services, which are used in both civilian and military operations (Box 2).[4]

- **Positioning, navigation and timing (PNT)** - sending users an accurate measure of their local time and location.[2,4]

The Parliamentary Office of Science and Technology, Westminster, London SW1A 0AA
02072192840 post@parliament.uk **parliament.uk/post** @POST_UK

Box 1: UK space and defence policy
Within Government, responsibility for space sits across a number of departments: the Ministry of Defence (MoD) (for military space policy); the Department for Business, Energy & Industrial Strategy (BEIS) and the UK Space Agency (for commerce and critical national infrastructure that is not defence-specific); and the Cabinet Office.[1] Following a Government review of space governance and structures, high-level policy and strategy functions are due to move from the UK Space Agency to BEIS by Autumn 2021.[25,26]

Over the next 10 years, the Government has committed around £5 bn to upgrade the SKYNET system of military communication satellites, and a further £1.4 bn for other space-based capabilities.[27] The Integrated Review outlined the Government's plans for an integrated approach across military and civil space policy,[27–29] including:

- A UK Space Command (launched in April 2021), to control and develop MoD space capabilities and to assist with coordinating commercial space operations
- Commercial facilities for launching satellites by 2022
- A Space Academy to train defence space specialists
- Developing a UK-built intelligence, surveillance and reconnaissance satellite constellation
- Developing other space capabilities, such as systems to track space debris and to investigate incidents in space.

- **Communication** - providing television, broadband internet, telephone and data transfer services.[30]
- **Observation and sensing** - imaging the Earth and space using a number of different sensors (POSTnote 566).[31–34]

UK access to space-based assets

UK access to certain satellite data and communications services comes via UK-owned assets (including those managed by companies on behalf of the Government). However, most services are provided through agreements with allied nations.[35]

UK-owned assets

Communications

In May 2021, 241 satellites were owned or operated by UK-based organisations.[14,36] The OneWeb constellation accounted for 182 of these, which is part-owned by the UK Government.[37] The British Armed Forces and UK allies receive global communications coverage through the SKYNET system of six satellites, which is owned and operated on behalf of the MoD by Airbus Defence and Space.[29,38] SKYNET is being upgraded, including plans to launch an extra satellite in 2025 (Box 1).[39]

Earth observation (EO)

The RAF launched Carbonite-2 in 2018, a demonstration mission for EO satellite technology.[40] The Government plans to increase UK EO capabilities with a new intelligence, surveillance and reconnaissance satellite constellation (Box 1).[27,41,42]

Launch facilities

Currently, the UK has no satellite launch capability and UK-based companies use facilities in other nations.[43] However, spaceports that can launch small satellites (under 180kg) are being developed in Scotland, Wales and Cornwall.[44–46]

Access via other states and international alliances

Positioning, navigation and timing

The UK relies on the US-owned Global Positioning System (GPS) for PNT services.[56] The EU is developing Galileo, its own global navigation satellite system, to gain greater control over its PNT services and an alternative if GPS fails (POSTbrief 37).[57,58] The UK left the Galileo programme after withdrawing from the EU.[59] It can still access Galileo's 'open' PNT services, but not the more resilient encrypted Public Regulated Service, intended for military and emergency services use.[60] The Government is investing £2 m to improve the resilience of UK PNT services and explore options for a UK satellite PNT system, under the Space Based PNT Programme.[61] An initial estimate made in 2018 suggested that a UK equivalent to Galileo could cost £3-5 bn.[62]

Earth observation

The UK continues to participate in the EU EO programme, Copernicus, which produces satellite data for many applications ranging from border security to climate monitoring.[63,63,64] The British Armed Forces get most of their EO data for satellite surveillance and reconnaissance from the US.[65]

Box 2: Example uses of satellites

Civilian applications

- **Emergency services**: satellite navigation services are used to locate and travel to incidents.[47]
- **Energy networks**: the national grid uses satellite timing services for electricity delivery.[48]
- **Financial transactions**: highly accurate timestamps are required for trading and audit purposes.[2,48]
- **Food and farming**: satellite navigation is used in food distribution and automated agricultural vehicles.[49,50]
- **Transport**: road, rail, air and sea transport all rely heavily on satellite navigation signals.[8]
- **Communications**: mobile phone networks, internet services and broadcasting use satellite networks.[48]
- **Research**: data from satellite-based sensors help to monitor air quality and changes in climate.[51,52]

Military applications

- **Navigation**: gives geographic guidance for personnel and for targeting precision weapons.[3]
- **Communications**: enables command and control, supports decision making and provides welfare services.[53]
- **Intelligence, surveillance and reconnaissance**: enables precision targeting of munitions, threat analysis, missile warning, and battle damage assessments.[3,54]
- **Weather monitoring**: provides information about conditions in areas of operations.[55]

Potential risks to satellites

Risks can vary between individual satellite missions.[66] Satellite services may be disrupted through unintentional damage, disruption or deliberate attacks by states or non-state actors.

Unintentional damage and disruption

Collisions with space debris or spacecraft

Space debris refers to all human-made objects in orbit around the Earth, or re-entering the atmosphere, that no longer have a function.[67] It includes defunct satellites, rocket stages used to launch satellites and small fragments from collisions, explosions or deterioration of active satellites.[68,69] The European Space Agency (ESA) estimates that there are roughly 34,000 objects larger than 10cm, 0.9 million (m) from 1 to 10cm, and 128 m from 1mm to 1cm.[70] Even small objects can be a serious risk, due to the high speeds at which they move.[71] The effects of a collision between a satellite and an object can vary from the loss of subsystems to its total destruction.

Collisions can create more debris. ESA reported an average of 12 debris creation events (caused by collisions, detachment of objects or explosions) every year for the past 20 years.[72] It has been suggested that if debris becomes sufficiently dense, a collision might trigger a cascade of further collisions, potentially rendering some orbits unusable.[73–75] As the number of satellites grows, the chances of them colliding with other spacecraft or debris also rises.[72] There are guidelines to avoid creating new debris, but it is difficult to determine responsibility for removing the vast amount of debris already in orbit (Box 3).[67,76]

Space weather
'Space weather' describes changes in the environmental conditions of the region of space close to the Earth, caused by radiation and material ejected from the Sun.[77] In an extreme space weather event, the Royal Academy of Engineering estimates that up to 10% of satellites could experience temporary outages lasting hours to days, with loss or disruption of satellite-enabled services.[78] Understanding of how often the Earth will experience an extreme space weather event is poor. The UK's National Risk Register gives a 1-5% chance of a severe space weather event occurring within the next year.[79,80]

Deliberate attacks

'Counterspace capabilities' can be used to target satellites, ground stations or other assets. There are four types: those using direct force to cause physical damage (kinetic physical), those that cause physical damage without touching the satellite (non-kinetic physical), electronic weapons, and cyber-attacks.[81]

Kinetic physical counterspace weapons
These weapons make direct physical contact with a satellite or ground station. They can be either 'direct ascent', where they are launched from the ground, or 'co-orbital', where they are placed in the Earth's orbit and manoeuvred towards an intended target.[81] The US, Russia, China, and India have all tested kinetic physical anti-satellite missiles against their own satellites in low-Earth orbit (Library Briefing 9261).[10,24,82–85]

There have been unconfirmed reports of China testing ballistic missiles that could reach geostationary orbit (36,000km above the Earth).[10,86,87] Technologies under development to service satellites in orbit, or to remove inactive satellites after use, might also be adapted to attack an adversary's satellite.[88,89] There are no known examples of kinetic counterspace weapons being used against an adversary's satellite.[10,90]

Non-kinetic physical counterspace weapons
These weapons cause physical damage to satellites or ground stations without making physical contact. Lasers can either temporarily blind a satellite's sensors or cause permanent damage by overheating the satellite's electronics.[81] The US, China and Russia are thought to be developing high energy lasers for anti-satellite use but there is no public evidence to suggest these are being used operationally.[10,91] High-power microwave weapons (HPMs) fire short bursts of microwave energy at a target satellite, damaging or destroying electrical systems.[92] The US has developed HPMs for terrestrial military use, but there is no publicly available evidence of it developing HPMs for use in space.[10] India recently announced plans to develop both laser and microwave-based weapons.[90]

Box 3: International governance of space
Nation states are responsible for their space activities, including those carried out by non-governmental entities such as companies.[93] Five UN treaties outline broad principles for space-related activities, the most significant of which is the Outer Space Treaty 1967.[94] There have been some calls for the laws governing the use of space to be updated.[95] The UK has proposed a UN General Assembly First Committee resolution on reducing space threats through norms, rules and responsible behaviour.[96,97]

Any person or organisation that operates, launches, or procures the launch of a satellite, must obtain authorisation from their national government.[93] The Civil Aviation Authority, which issues licences in the UK, requires operators to state the length of mission and method of de-orbiting after use.[98] The G7 nations have issued a statement recognising the growing hazard of space debris and committing to the safe and sustainable use of space.[99]

Electronic weapons
These target the radio signals that carry data to and from satellites. For example, jamming technology boosts background noise at the same frequency as the radio signals, preventing the receiver from distinguishing them from the noise. Spoofing involves an adversary sending a false signal to a satellite or ground station that appears to be genuine. This enables them to give satellites false information, or even false commands.[81]

The availability and relative low-cost of electronic jamming and spoofing technologies make electronic attacks accessible to both state and non-state actors.[90] There have been reports of suspected Russian spoofing of GPS, including within Russia, Crimea and Syria; and Russian jamming of GPS to disrupt the use of drones in Syria and the Ukraine.[100–103] There have also been reports of jamming and spoofing of ships' GPS signals at the Chinese port of Shanghai, leading to their locations being incorrectly reported to crew and other vessels.[104,105]

Cyber-attacks
Cyber-attacks can target satellites, ground systems, or end-user equipment such as GPS receivers. They may involve monitoring data traffic patterns, intercepting data, or inserting false or corrupt data into the system.[81,106–109] Cyber-attacks require in-depth knowledge of the target systems, but do not necessarily need significant resources and can be contracted out, for example to organised crime groups or terrorists.[81,110,111]

Attribution of incidents

A kinetic physical counterspace attack would likely be easily observable and attributable to its source.[112] By contrast, non-kinetic physical attacks can be more difficult to attribute. The approximate location of a laser attack could be traced, but HPMs are difficult to trace back to their origin.[81] Electronic attacks can be hard to detect and distinguish from accidental interference, making identification and attribution challenging. In addition, once jamming and spoofing are turned off, communications return to normal.[81,113] Cyber-attacks can be difficult to attribute and may go undetected for long periods.[106]

A further challenge for attribution is that satellite systems are often 'dual use', because they can be used for both civilian and military activities.[114,115] A purported civilian satellite might be used in a military capacity without an adversary realising.[116]

Difficulties with attributing attacks, combined with forms of attack that are reversible or non-destructive, make it easier for adversaries to use space to pursue their political goals through "sub-threshold" activities. These are activities that the perpetrator believes fall below the threshold of overt conflict.[117–119] For example, Norway has accused Russia of disrupting navigation systems during NATO training exercises, also affecting commercial aircraft flying in the area.[120,121]

Mitigating the risks to satellites

The MoD tests its dependence on space-based assets through classified audits and simulations of military operations.[25] It does not publish details about UK space defence capabilities. Space situational awareness (Box 4) provides a picture of the space environment and is a key tool for identifying potential risks. Other approaches may also help to reduce the risks posed to a satellite from unintentional damage or deliberate attack, and to improve the resilience of critical services.[81] Appropriate mitigation measures can vary between satellite missions.[66]

Reducing the risk of unintentional damage

Space debris removal

Academic studies have modelled a range of potential space debris removal mechanisms. For example:

- lasers positioned on the ground or on nearby spacecraft to push debris out of orbit
- nets, harpoons or sails thrown from a satellite to trap debris
- satellites with robotic arms to collect debris.[122–125]

Most of these methods have not been tested in space, but the RemoveDEBRIS project successfully trialled two techniques - a net and a harpoon - in orbit in 2018.[126,127] Astroscale, a debris removal company, is also developing technology to remove retired satellites fitted with a specific attachment.[128]

Improving resilience to space weather

Shielding materials can be used to protect satellites from solar radiation.[129] With sufficient notice, operators can lower satellite power to reduce the damage done by a space weather event.[130] The UK Government plans to publish a space weather strategy in 2021 and is investing £20m in the SWIMMR project to improve space weather prediction and monitoring.[106,131,132]

Reducing the risk of deliberate attack

Technical defences

Technical features can be incorporated into the physical structure or software of a satellite system to make it more difficult to attack. In some cases, these may add to the weight and cost of the satellite. Example features include:

- Surrounding electronics with protective materials to shield against high-power microwave attacks
- Fitting filters over satellite sensors to protect against lasers
- Using directional antenna on ground stations, or changing satellite signal frequency, to mitigate electronic attacks
- Encrypting satellite signals, which can prevent a cyber intrusion. This is standard practice with military systems but is not always done with commercial systems.
- 'Air-gapping' a satellite system by separating it from the public internet, to avoid cyber-attacks (which is difficult for satellite systems that produce data for public use).[30,81,133]

Box 4: Space situational awareness

Space situational awareness (SSA) is the ability to observe, track and predict the movement of objects in orbit.[134] This helps to reduce the risk of satellites colliding with space debris or other spacecraft. SSA can also monitor other space users' behaviour. A closely related term - space domain awareness (SDA) - is sometimes used, particularly in defence contexts, and tends to include a focus on intelligence activities.[135–138] The British Armed Forces obtain SSA data from the US Space Surveillance Network (SSN), which consists mainly of ground-based telescopes and radar sensors. The UK contributes some data to SSN via a radar facility in Yorkshire.[139,140,141] The National Space Operations Centre aims to enhance the UK's ability to collect and respond to SDA data.[27,142]

Export controls

The dual-use nature of satellites means that the export of certain parts requires a license, under international export control agreements.[143,144] The Integrated Review stated that the UK will seek to ensure that export control systems reduce the proliferation of space weapons and dual-use technologies.[28]

Improving the resilience of critical services

The resilience of satellite networks can be improved through the way that they are designed and operated. If satellites are disrupted, access to terrestrial alternatives can help to maintain access to critical services.[13,145]

Use of multiple satellites

A swarm approach - where one system is made up of a network of multiple satellites - can help to make both military and civil satellite systems more resilient.[146–148] If one satellite fails, others can maintain the same services.[149]

Modifying satellite operations

Satellites can be operated strategically to ensure the continued provision of services. If one satellite is damaged, a new satellite can be deployed in its place.[150] Satellites can be manoeuvred in order to avoid unguided kinetic physical counterspace weapons, but guided missiles or other satellites would be harder to evade. Satellites can avoid detection by using radar-absorbing coatings or jamming adversaries' detection sensors.[81,151]

Enhancing cyber-resilience

A stakeholder consultation by Chatham House suggested approaches for improving cyber-resilience. These included developing industry-led standards; increasing cooperation internationally and between different stakeholder groups (e.g. operators, government agencies and manufacturers); and improving understanding of security requirements and vulnerabilities, across the space and cyber communities.[111,152]

Terrestrial alternatives

The £2m National Timing Centre is developing a network of atomic clocks across the UK, as a terrestrial alternative to satellite-based timing signals.[153] However, terrestrial alternatives may not always be available, and have their own vulnerabilities. Training can help personnel to understand the dependences and vulnerabilities of systems and to obtain the skills needed to operate without access to satellite services.[13]

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Lucy Smythe for researching this briefing, to the Engineering and Physical Sciences Research Council for funding her parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Lydia Harriss.

1. UK Space Agency (2015). *National Space Policy.*
2. GO Science (2018). *Satellite-derived Time and Position: A study of critical dependencies.*
3. Ministry of Defence (2010). *The UK Military Space Primer*.
4. Defense Intelligence Agency (2019). *Challenges to Security in Space*.
5. UK Space Agency (2021). *UK space industry: size and health report 2020.*
6. This estimate indicates the total value of output of those UK industries that are supported by satellite services from both UK and non-UK satellites. It is not a valuation of the economic value contributed by satellite services. It does not cover the full UK economy, but reflects the coverage of the Office for National Statistic's Annual Business Survey and is limited to the UK's Non-Financial Business Economy. It excludes: financial and insurance, public administration and defence, public provision of education, public provision of health and all medical and dental practice activities.
7. Green et al. (2016). Building space weather resilience in the finance sector. *UCL Public Policy.*
8. London Economics (2017). *The economic impact on the UK of a disruption to GNSS.*
9. Harrison (2013). Unpacking the Three C's: Congested, Competitive, and Contested Space. *Astropolitics*, Vol 11, pgs123–131.
10. Weeden and Samson. (2021). *Global Counterspace Capabilities*. Secure World Foundation
11. The Economist [online]. Africa is blasting its way into the space race. Accessed 21/07/2021
12. Warrick (2021). Russia is preparing to supply Iran with an advanced satellite system that will boost Tehran's ability to surveil military targets, officials say. *Washington Post* Accessed 13/08/2021
13. Defence Select Committee (29/09/2020) *The Integrated Review- Threats, Capabilities and Concepts.* Oral Evidence Alexandra Stickings, Todd Harrison, Bleddyn Bowen
14. Union of Concerned Scientists [online] Satellite Database. Accessed 09/07/2021
15. Murtaza et al. (2020). Orbital Debris Threat for Space Sustainability and Way Forward (Review Article). *IEEE Access*, Vol 8, pgs61000–61019.
16. Boley et al. (2021). Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere and on Earth. *Scientific Reports*, Vol 11, pgs10642.
17. Figure calculated using data from the Union of Concerned Scientists Satellite Database, updated 1st May 2021. Data included satellites with a mix of users (e.g. commercial/government and commercial/military), which encompasses global navigation satellite systems such as GPS.
18. Long (2021) Amazon Internet Program, Project Kuiper, to Launch Satellite. *Government Technology* Accessed 19/06/2021
19. Rainbow (2021) OneWeb adds 36 satellites to broadband constellation as deployment accelerates. *Space News* Accessed 15/06/2021
20. Space.com [online] Starlink: SpaceX's satellite internet project. Accessed 29/06/2021
21. Airbus [online] Mega-constellations in space: revolutionising the satellite industry. Accessed 13/08/2021
22. Housley, C. *et al.* (2021). The UK Space Industry. House of Commons Library.
23. Commons PQ (2020). UIN 3707: Defence.
24. Mills et al. (2021). The militarisation of space. House of Commons library.
25. Private communication between POST and the MoD.
26. Titcomb (2021). Shake up for UK's space plans after OneWeb row. *The Telegraph*. Accessed 09/07/2021
27. Ministry of Defence (2021). *Defence in a Competitive Age*.
28. Cabinet Office (2021). *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*.
29. Ministry of Defence [online]. UK Space Command. Accessed 05/07/2021
30. Wright et al. (2005). *The Physics of Space Security*. American Academy of Arts and Sciences.
31. Fu et al. (2020). *Remote Sensing Satellites for Digital Earth*.
32. UK Space Agency Space for Smarter Government [online] Earth Observation. Accessed 23/06/2021
33. Nieves-Chinchilla et al. (2020). International Coordination and Support for SmallSat-Enabled Space Weather Activities. *Space Weather*, Vol 18.
34. European Space Agency [online] Monitoring space weather. Accessed 21/06/2021
35. Bowen (2018). British strategy and outer space: A missing link? *The British Journal of Politics and International Relations*, Vol 20, pgs323–340.
36. Data from the Union of the Concerned Scientists Satellite Database, updated 1st May 2021. The figure of 241 includes satellites jointly owned with international agencies, or with companies or governments based in other countries.
37. GOV.UK [online] UK government secures satellite network OneWeb. Accessed 14/06/2021
38. GOV.UK [online] Defence Secretary announces boost for multi-billion-pound SKYNET 6 programme. Accessed 20/05/2021
39. Airbus [online] Airbus signs contract with UK Ministry of Defence for Skynet 6A satellite. Accessed 14/06/2021
40. CPI (2018). SatMagazine.
41. GOV.UK [online] Lift-off: Satellite launched into space on RAF mission. Accessed 18/06/2021
42. UK Space Agency (2019). *UK EO Technology Strategy*.
43. UK Space Agency (2021). *UK Registry of Space Objects*.
44. UK Space Agency [online] A guide to the UK's commercial spaceports. Accessed 04/06/2021.
45. Hutton [online]. When will UK spaceports be ready for lift-off? House of Commons Library. Accessed 04/06/2021
46. Mabrouk [online] What are SmallSats and CubeSats? *NASA*. Accessed 21/06/2021.
47. Davies (2017). The satellite security blind spot: what it means for paramedics on the frontline. *Journal Of Paramedic Practice*.
48. Falletti *et al.* (2019). Synchronization of Critical Infrastructures Dependent Upon GNSS: Current Vulnerabilities and Protection Provided by New Signals. *IEEE Systems Journal*, Vol 13, pgs2118–2129.
49. Yang (2018). High resolution satellite imaging sensors for precision agriculture. *Frontiers of Agricultural Science and Engineering*, Vol 5, pgs393–405.
50. POST UK (2015). *Precision Farming*.

51. Met Office [online] Observations from space. Accessed 26/05/2021
52. Science and Technology Facilities Council [online] Earth Observation. Accessed 26/05/2021
53. Lueschow et al. (2020). Satellite Communication for Security and Defense in *Handbook of Space Security*. pgs779–796.
54. Valentino, G. [online] Using the Space Domain. *Joint Air Power Competence Centre*. Accessed 14/06/2021
55. Bowen (2021). *The Integrated Review and UK Spacepower: The Search for Strategy*. Freeman Air & Space Institute.
56. GPS.gov [online] The Global Positioning System. Accessed 10/06/2021
57. Prime Minister's Office (2020). Our approach to the Future Relationship with the EU. UK Government
58. Fiott (2020). *The European space sector as an enabler of EU strategic autonomy*. Policy Department for External Relations, European Parliament.
59. Wallace (2020). Brexit deal secures UK access to European research funds. *Science*.
60. GOV.UK [online] UK involvement in the EU Space Programme. Accessed 22/06/2021.
61. GOV.UK [online] UK space sector wins over £2 million to help develop options for a national position, navigation and timing space system. Accessed 06/07/2021.
62. Commons PQ (2020). UIN HL2116: Global Navigation Satellite Systems.
63. POST (2020). *POSTbrief 37: Key EU space programmes*.
64. Secretary of State for Foreign, Commonwealth and Development Affairs (2021). *Trade and Cooperation Agreement.* European Commission.
65. Hilborne, M. and Presley M. (2020). *Towards a UK Space Surveillance Policy: Protecting and growing UK equities within space.* The Policy Institute, Kings College London.
66. National Aeronautics and Space Administration (2015). Security Threats against Space Missions.
67. United Nations Office for Outer Space Affairs (2010). Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space.
68. Mark et al. (2019). Review of Active Space Debris Removal Methods. *Space Policy*, Vol 47, pgs194–206.
69. POST UK (2010). *Space Debris*.
70. Defence Select Committee (13/07/2021). *Space Defence.* Oral Evidence Mark Hilborne and Mark Presley.
71. European Space Agency [online] Space debris by the numbers. Accessed 21/07/2021
72. European Space Agency [online] The current state of space debris. Accessed 21/06/2021.
73. Newman et al. (2018). Space Sustainability: Reframing the Debate. *Space Policy*, Vol 46, pgs30–37.
74. David (2021) Space Junk Removal Is Not Going Smoothly. *Scientific American*. Accessed 15/08/2021.
75. Commons PQ (2021). UIN 2402: Space Debris.
76. Haroun et al. (2021). Toward the Sustainability of Outer Space: Addressing the Issue of Space Debris. *New Space*, Vol 9, pgs63–71.
77. POST UK (2010). *Space weather.*
78. Hands et al. (2018). Radiation Effects on Satellites During Extreme Space Weather Events. *Space Weather*, Vol 16, pgs1216–1226.
79. HM Government (2020). National Risk Register.
80. Elvidge et al. (2018). Using Extreme Value Theory for Determining the Probability of Carrington-Like Solar Flares. *Space Weather*, Vol 16, pgs417–421.
81. Harrison et al. (2021). *Defense against the dark arts in space: protecting space systems from counterspace weapons*. Center for Strategic and International Studies
82. European Space Agency [online] Low Earth orbit. Accessed 18/06/2021
83. Kan (2007). *China's Anti-Satellite Weapon Test*. Library of Congress Washington DC Congressional Research Service.
84. Ministry of External Affairs, Government of India (2019). Frequently Asked Questions on Mission Shakti, India's Anti-Satellite Missile test conducted on 27 March, 2019.
85. US Space Command Public Affairs Office (2020). Russia tests direct-ascent anti-satellite missile. *United States Space Command*.
86. Office of the Secretary of Defense (2020). *Military and security developments involving the People's Republic of China.*
87. European Space Agency [online] The geostationary orbit. Accessed 22/06/2021.
88. Northrop Grumman [online] Northrop Grumman and Intelsat Make History with Docking of Second Mission Extension Vehicle to Extend Life of Satellite. Accessed 16/08/2021.
89. Martin et al. (2019). Exploring the Legal Challenges of Future on-Orbit Servicing Missions and Proximity Operations. *Journal Space Law*, Vol 43, pgs196–222.
90. Harrison et al. (2021). *Space Threat Assessment 2021*. Center for Strategic and International Studies.
91. Gao et al. (2013). Development of space-based laser weapon systems. *Chinese optics*, Vol 6,pgs 810–817.
92. McGonegal (2020). *High Power Microwave Weapons: Disruptive Technology for the Future.* Air Command and Staff.
93. GOV.UK [online] Spaceflight legislation and guidance. Accessed 15/08/2021
94. United Nations Office for Outer Space Affairs (2017). International Space Law: United Nations Instruments.
95. Johnson-Freese (2017). Build on the outer space treaty. *Nature*, Vol 550, pgs182–184.
96. GOV.UK [online] UK push for landmark UN resolution to agree responsible behaviour in space. Accessed 19/05/2021.
97. UN General Assembly (2020). Reducing space threats through norms, rules and principles of responsible behaviours.
98. UK Government (2020). Guidance for launch and return operator licence applicants and licensees.
99. GOV.UK [online] G7 nations commit to the safe and sustainable use of space. Accessed 14/06/2021.
100. BBC [online] Study maps 'extensive Russian GPS spoofing'. Accessed 26/08/2021
101. Kube (2018). Russia Jamming GPS Signals in Syria to Counter US Drones - NBC News. *Resilient Navigation and Timing Foundation*.
102. C4ADS (2019). *Above Us Only Stars: Exposing GPS spoofing in Russia and Syria.* C4ADS innovation for peace.
103. Goward [online] Russia ramps up GPS jamming along with troops at Ukraine border. *GPS World*. Accessed 16/08/2021

104. Gordon et al. (2018). China Installed Military Jamming Equipment on Spratly Islands, U.S. Says. *Wall Street Journal*.
105. Harris (2019). Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai. *MIT Technology Review*.
106. Pavur et al. (2019). The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. *11th International Conference on Cyber Conflict (CyCon)*. Vol 900, pgs1–18.
107. Reinsch et al. (2011). US-China Economic and Security Review Commission. US Congress.
108. Flaherty et al. [online] Chinese hack U.S. weather systems, satellite network. *Washington Post*. Accessed 15/08/2021
109. Manulis et al. (2021). Cyber security in New Space. *International Journal of Information Security*, Vol 20, pgs287–311.
110. Handberg (2017). Is space war imminent? Exploring the possibility. *Comparative Strategy*, Vol 36,pgs 413–425.
111. Livingstone and Lewis. (2016). *Space, the Final Frontier for Cybersecurity?* Chatham House.
112. Grego (2012). A History of Anti-Satellite Programs. *Union of Concerned Scientists*.
113. Lindsay (2015) Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, *Journal of Cybersecurity,* Vol 1, pgs53-63.
114. Finocchio et al. (2008). *Aerospace Technologies and Applications for Dual Use*.
115. Pražák (2021). Dual-use conundrum: Towards the weaponization of outer space? *Acta Astronautica*, Vol 187, pgs397-405.
116. Johnson-Freese et al. (2019). The Outer Space Treaty and the weaponization of space. *Bulletin of the Atomic Scientists*, Vol 75, pgs137–141.
117. Morris et al. (2019). *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. RAND Corporation.
118. Popp *et al.* (2016). *The Characterization and Conditions of the Gray Zone.*
119. Defence Select Committee (29/09/2020) *The Integrated Review- Threats, Capabilities and Concepts.* Oral Evidence Alexandra Stickings, Todd Harrison and Bleddyn Bowen
120. Adomaitis et al. [online] Norway says it proved Russian GPS interference during NATO exercises. *Reuters*. Accessed 08/06/2021.
121. Staalesen [online] Norway requests Russia to halt GPS jamming in borderland. *The Independent Barents Observer*. Accessed 09/06/2021
122. Soulard et al. (2014). ICAN: A novel laser architecture for space debris removal. *Acta Astronautica*, Vol 105, pgs192–200.
123. Guang et al. (2012). Space Tether Net System for Debris Capture and Removal. *4th International Conference on Intelligent Human-Machine Systems and Cybernetics*. Vol 1, pgs257–261.
124. Kelly et al. (2018). TugSat: Removing Space Debris from Geostationary Orbits Using Solar Sails. *Journal of Spacecraft and Rockets*, Vol 55, pgs437–450.
125. Dubanchet et al. (2015). Modeling and control of a space robot for active debris removal. *CEAS Space Journal*, Vol 7, pgs203–218.
126. Forshaw et al. (2020). The active space debris removal mission RemoveDebris. Part 1: From concept to launch. *Acta Astronautica*, Vol 168, pgs293–309.
127. Aglietti et al. (2020). The active space debris removal mission RemoveDebris. Part 2: In orbit operations. *Acta Astronautica*, Vol 168, pgs310–322.
128. Astroscale [online] Astroscale UK Signs £2.5 Million Agreement to Develop Space Debris Removal Technology Innovations with OneWeb. Accessed 06/06/2021.
129. Atxaga et al. (2012). Radiation shielding of composite space enclosures. 63rd International Astronautical Congress.
130. NASA [online] *State of the Art: Small Spacecraft Technology*. Accessed 01/07/2021.
131. UKRI STFC RAL [online] Space SWIMMR (Space Weather Instrumentation, Measurement, Modelling and Risk). Accessed 01/07/2021.
132. Commons PQ (2021). UIN 1168: Solar Events.
133. Zeynali et al. (2012). Shielding protection of electronic circuits against radiation effects of space high energy particles. *Advances in Applied Science Research*, Vol 3, pgs446–451.
134. Space Foundation (2019). The Space Briefing Book.
135. Holzinger and Jah (2018). Challenges and Potential in Space Domain Awareness. *Journal of Guidance, Control, and Dynamics*, Vol 41, pgs15–18.
136. di Mare (2021). The Role of Space Domain Awareness. in *Joint Air Power Competence Centre*.
137. Erwin [online] Air Force: SSA is no more; it's 'Space Domain Awareness'. *SpaceNews*. Accessed 24/08/2021.
138. Jah (2016). Space Surveillance, Tracking, and Information Fusion for Space Domain Awareness. NATO Science and Technology Organisation. Lecture Series SCI-292-LS.
139. Ash et al. (2018). A Summary of 5-Eyes Research Collaboration into SSA.
140. Stickings (2019). *The Future of EU–US Cooperation in Space Traffic Management and Space Situational Awareness.* Chatham House.
141. Roberts [online] Popular Orbits 101. *Aerospace Security*. Accessed 22/06/2021.
142. UN Office for Outer Space Affairs (2021). *Promoting Space Sustainability.*
143. GOV.UK [online] UK Strategic Export Control Lists. Accessed 23/06/2021.
144. Horton (2018). Space, the International Export Control Regimes and the UK's Strategic Export Controls. Department for International Trade.
145. Ministry of Defence (2020). Joint Concept Note 1/20 Multi-Domain Integration. *Development, Concepts and Doctrine Centre*,
146. Febvre (2019). A Swarm-based Approach to Hardening Future Military Satellite Communication Assets.
147. Dono et al. (2018). Propulsion trade studies for spacecraft swarm mission design. *2018 IEEE Aerospace Conference*.
148. Kodheli et al. (2021). Satellite Communications in the New Space Era: A Survey and Future Challenges. *IEEE Communications Surveys Tutorials*, Vol 23, pgs70–109.
149. Chang [online] Protecting next-generation Military Satellite Communications with an innovative disaggregation approach. *Air and Space Power Review*. Accessed 23/06/2021.
150. Office of the Assistant Secretary of Defense for Homeland Defense & Global Security (2015). *Space Domain Mission Assurance: A Resilience Taxonomy.*

151. Zhu et al. (2016). Optical Stealth Design of Satellite. 2016 International Conference on Mechatronics Engineering and Information Technology.
152. King *et al.* (2020). Cybersecurity Threats in Space: A Roadmap for Future Policy. *Science and Technology Innovation Program*.
153. NPL [online] National Timing Centre Programme. Accessed 24/06/2021.